Order Code 98-326

Report for Congress
Received through the CRS Web

Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping

Updated January 13, 2003

Gina Stevens
Legislative Attorney
American Law Division

Charles Doyle
Senior Specialist
American Law Division

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
13 JAN 2003		**00-00-2003 to 00-00-2003**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Congressional Research Service,Library of Congress,101 Independence Ave., SE,Washington,DC,20540-7500**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**86**	

Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping

Summary

This report provides an overview of federal law governing wiretapping and electronic eavesdropping. It also surveys state law in the area and contains a bibliography of legal commentary.

It is a federal crime to wiretap or to use a machine to capture the communications of others without court approval, unless one of the parties has given their prior consent. It is likewise a federal crime to use or disclose any information acquired by illegal wiretapping or electronic eavesdropping. Violations can result in imprisonment for not more than 5 years; fines up to $250,000 (up to $500,000 for organizations); in civil liability for damages, attorneys fees and possibly punitive damages; in disciplinary action against any attorneys involved; and in suppression of any derivative evidence. Congress has created separate but comparable protective schemes for electronic mail (e-mail) and against the surreptitious use of telephone call monitoring practices such as pen registers and trap and trace devices.

Each of these protective schemes comes with a procedural mechanism to afford limited law enforcement access to private communications and communications records under conditions consistent with the dictates of the Fourth Amendment. The government has been given even more narrowly confined authority to engage in wiretapping and electronic eavesdropping in the name of foreign intelligence gathering in the Foreign Intelligence Surveillance Act.

Contents

Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping

Introduction[1]

Depending on one's perspective, wiretapping and electronic eavesdropping are either "dirty business," essential law enforcement tools, or both. This is a very general overview of the federal statutes that proscribe wiretapping and electronic eavesdropping and of the procedures they establish for law enforcement and foreign intelligence gathering purposes. Special attention is given to three particularly troublesome areas of the law: digital telephony, cell phone interception, and encryption. Although the specifics of state law are beyond the scope of this report, citations to related state statutory provisions and a selected bibliography of legal materials have been appended.

Background

---

[1] Portions of this report draw upon a series of earlier reports, no longer available, entitled: *Wiretapping and Electronic Surveillance: A Brief Discussion of Pertinent Supreme Court Cases, A Summary and Compilation of Federal State Statutes, and a Selected Legal Bibliography* (1970); *Wiretapping and Electronic Surveillance: A Brief Discussion of Pertinent Supreme Court Cases, A Summary and Compilation of Federal State Statutes, and a Selected Legal Bibliography* (1971); *Wiretapping and Electronic Surveillance: Federal and State Statutes* (1974); *Taps and Bugs: A Compilation of Federal and State Statutes Governing the Interception of Wire and Oral Communications* (1981); *The Interception of Communications: A Legal Overview of Bugs and Taps* (1988); *Wiretapping & Electronic Surveillance: The Electronic Communications Privacy Act and Related Matters* (1992); *Taps, Bugs & Telephony: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping* (1998); *Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping* (2001).

As used in this report "electronic eavesdropping" refers to the use of hidden microphones, recorders and any other mechanical or electronic means of ongoing capturing communications, other than wiretapping (tapping into telephone conversations). In previous versions of this report and other earlier writings, it was common to use a more neutral term – electronic surveillance – at least when referring to law enforcement use. Unfortunately, continued use of the term "electronic surveillance" rather than "electronic eavesdropping" risks confusion with forms of surveillance that either have individualistic definitions (e.g., "electronic surveillance" under the Foreign Intelligence Surveillance Act, 18 U.S.C. 1801(f)), that involve surveillance that does not capture conversation (*e.g.*, thermal imaging or electronic tracking devices), or that may or may not capture conversation (*e.g.*, video surveillance which when it does capture conversation is covered by the law governing electronic eavesdropping, *see United States v. Williams*, 124 F.3d 411 (3d Cir. 1997)).

At common law, "eavesdroppers, or such as listen under walls or windows, or the eaves of a house, to hearken after discourse, and thereupon to frame slanderous and mischievous tales, are a common nuisance and presentable at the court-leet; or are indictable at the sessions, and punishable by fine and finding of sureties for [their] good behavior," 4 BLACKSTONE, COMMENTARIES ON THE LAWS OF ENGLAND, 169 (1769).

Although early American law proscribed common law eavesdropping, the crime was little prosecuted and by the late nineteenth century had "nearly faded from the legal horizon."[2] With the invention of the telegraph and telephone, however, state laws outlawing wiretapping or indiscretion by telephone and telegraph operators preserved the spirit of the common law prohibition in this country.

Congress enacted the first federal wiretap statute as a temporary measure to prevent disclosure of government secrets during World War I.[3] Later, it proscribed intercepting and divulging private radio messages in the Radio Act of 1927,[4] but did not immediately reestablish a federal wiretap prohibition. By the time of the landmark Supreme Court decision in *Olmstead*, however, at least forty-one of the forty-eight states had banned wiretapping or forbidden telephone and telegraph employees and officers from disclosing the content of telephone or telegraph messages or both.[5]

Olmstead was a Seattle bootlegger whose Prohibition Act conviction was the product of a federal wiretap. He challenged his conviction on three grounds, arguing unsuccessfully that the wiretap evidence should have been suppressed as a violation of either his Fourth Amendment rights, his Fifth Amendment privilege against self-incrimination, or the rights implicit in the Washington state statute that outlawed wiretapping.

---

[2] "Eavesdropping is indictable at the common law, not only in England but in our states. It is seldom brought to the attention of the courts, and our books contain too few decisions upon it to enable an author to define it with confidence. . . . It never occupied much space in the law, and it has nearly faded from the legal horizon." 1 BISHOP, COMMENTARIES ON THE CRIMINAL LAW, 670 (1882).

[3] 40 Stat.1017-18 (1918)("whoever during the period of governmental operation of the telephone and telegraph systems of the United States . . . shall, without authority and without the knowledge and consent of the other users thereof, except as may be necessary for operation of the service, tap any telegraph or telephone line . . . or whoever being employed in any such telephone or telegraph service shall divulge the contents of any such telephone or telegraph message to any person not duly authorized or entitled the receive the same, shall be fined not exceeding $1,000 or imprisoned for not more than one year or both"); 56 *Cong.Rec.* 10761-765 (1918).

[4] 44 Stat. 1172 (1927)(". . . no person not being authorized by the sender shall intercept any message and divulge or publish the contents, substance, purpose, effect, or meaning of such intercepted message to any person . . .").

[5] *Olmstead* v. *United States*, 277 U.S. 438, 479-80 n.13 (1928)(Brandeis, J., dissenting). *Olmstead* is remembered most today for the dissents of Holmes and Brandeis, but for four decades it stood for the view that the Fourth Amendment's search and seizure commands did not apply to government wiretapping accomplished without a trespass onto private property

For a majority of the Court, writing through Chief Justice Taft, Olmstead's Fourth Amendment challenge was doomed by the absence of "an official search and seizure of his person, or such a seizure of his papers or his tangible material effects, or an actual physical invasion of his house or curtilage[6] for the purposes of making a seizure," 277 U.S. at 466.[7]

Chief Justice Taft pointed out that Congress was free to provide protection which the Constitution did not.[8] Congress did so in the 1934 Communications Act by expanding the Radio Act's proscription against intercepting and divulging radio communications so as to include intercepting and divulging radio or wire communications.[9]

The Federal Communications Act outlawed wiretapping, but it said nothing about the use of machines to surreptitiously record and transmit face to face conversations.[10] In the absence of a statutory ban the number of surreptitious recording cases decided on Fourth Amendment grounds surged and the results began to erode *Olmstead*'s underpinnings.[11]

---

[6] Curtilage originally meant the land and buildings enclosed by the walls of a castle; in later usage it referred to the barns, stables, garden plots and the like immediately proximate to a dwelling; it is understood in Fourth Amendment parlance to describe that area which "harbors those intimate activities associated with domestic life and the privacies of the home," *United States v. Dunn*, 480 U.S. 294, 301 n.4 (1987).

[7] Olmstead had not been compelled to use his phone and so the Court rejected his Fifth Amendment challenge. 277 U.S.C. at 462. Any violation of the Washington state wiretap statute was thought insufficient to warrant the exclusion of evidence, 277 U.S. at 466-68. Justice Holmes in his dissent tersely characterized the conduct of federal wiretappers as "dirty business," 277 U.S. at 470. The dissent of Justice Brandeis observed that the drafters of the Constitution "conferred as against the Government, the right to be let alone – the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the Government against privacy of the individual whatever the means employed, must be deemed in violation of the Fourth Amendment," 277 U.S. at 478-79.

[8] "Congress may of course protect the secrecy of telephone messages by making them, when intercepted inadmissible in evidence in federal criminal trials, by direct legislation," 277 U.S. at 465.

[9] 48 U.S.C. 1103-4 (1934), 47 U.S.C. 605 (1940 ed.). The Act neither expressly condemned law enforcement interceptions nor called for the exclusion of wiretap evidence, but it was read to encompass both, *Nardone v. United States*, 302 U.S. 379 (1937); *Nardone v. United States*, 308 U.S. 321 (1939).

[10] Section 605 did ban the interception and divulgence of radio broadcasts but it did not reach the radio transmission of conversations that were broadcast unbeknownst to all of the parties to the conversation. Late in the game, the FCC supplied a partial solution when it banned the use of licensed radio equipment to overhear or record private conversation without the consent of all the parties involved in the conversation, 31 *Fed.Reg.* 3400 (March 4, 1966), amending then 47 C.F.R. §§2.701, 15.11. The FCC excluded "operations of any law enforcement offices conducted under lawful authority," *id.*

[11] The volume of all Fourth Amendment cases calling for Supreme Court review increased dramatically after *Mapp v. Ohio*, 367 U.S. 643 (1961), acknowledged the application of the Fourth Amendment exclusionary rule to the states.

Erosion, however, came slowly. Initially the Court applied *Olmstead*'s principles to these electronic eavesdropping cases. Thus, the use of a dictaphone to secretly overhear a private conversation in an adjacent office offended no Fourth Amendment precipes because no physical trespass into the office in which the conversation took place had occurred, *Goldman v. United States*, 316 U.S. 129 (1942). Similarly, the absence of a physical trespass precluded Fourth Amendment coverage of the situation where a federal agent secretly recorded his conversation with a defendant held in a commercial laundry in an area open to the public, *On Lee v. United States*, 343 U.S. 747 (1952). On the other hand, the Fourth Amendment did reach the government's physical intrusion upon private property during an investigation, as for example when they drove a "spike mike" into the common wall of a row house until it made contact with a heating duct for the home in which the conversation occurred, *Silverman v. United States*, 365 U.S. 505 (1961).

Silverman presented something of a technical problem, because there was some question whether the spike mike had actually crossed the property line of the defendant's town house when it made contact with the heating duct. The Court declined to rest its decision on the technicalities of local property law, and instead found that the government's conduct had intruded upon privacy of home and hearth in a manner condemned by the Fourth Amendment, 365 U.S. at 510-12.[12]

---

[12] "The absence of a physical invasion of the petitioner's premises was also a vital factor in the Court's decision in *Olmstead v. United States* . . . . In holding that the wiretapping there did not violate the Fourth Amendment, the Court noted that the insertions were made without trespass upon any property of the defendants. They were made in the basement of the large office building. The taps from house lines were made in the streets near the houses. 277 U.S. at 457. There was no entry of the houses or offices of the defendants. 277 U.S. at 464. Relying upon these circumstances, the Court reasoned that the intervening wires are not part of (the defendant's) house or office any more than are the highways along which they are stretched. 277 U.S. at 465.

"Here, by contrast, the officers overheard the petitioners' conversations only by usurping part of the petitioners' house or office – a heating system which was an integral part of the premises occupied by the petitioners, a usurpation that was effected without their knowledge and without their consent. In these circumstances we need not pause to consider whether or not there was a technical trespass under the local property law relating to party walls. Inherent Fourth Amendment rights are not inevitably measurable in terms of ancient niceties of tort or real property law . . . .

"The Fourth Amendment, and the personal rights which it secures, have a long history. At the very core stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion . . . This Court has never held that a federal officer may without warrant and without consent physically entrench into a man's office or home, there secretly observe or listen, and relate at the man's subsequent criminal trial what was seen or heard.

"A distinction between the dictaphone employed in Goldman and the spike mike utilized here seemed to the Court of Appeals too fine a one to draw. The court was unwilling to believe that the respective rights are to be measured in fractions of inches. But decision here does not turn upon the technicality of a trespass upon a party wall as a matter of local law. It is based upon the reality of an actual intrusion into a constitutionally protected area. What the Court said long ago bears repeating now: It may be that it is the obnoxious thing in its mildest and least repulsive form; but illegitimate and unconstitutional practices get their first footing in that way, namely, by silent approaches and slight deviations from legal modes of procedure. *Boyd v. United States*, 116 U.S. 616, 635. We find no occasion to re-examine Goldman here, but we decline to go beyond it, by even a fraction of an inch," 365 U.S. at

Each of these cases focused upon whether a warrantless trespass onto private property had occurred, that is, whether the *means* of conducting a search and seizure had been so unreasonable as to offend the Fourth Amendment. Yet in each case, the object of the search and seizure had been not those tangible papers or effects for which the Fourth Amendment's protection had been traditionally claimed, but an intangible, a conversation. This enlarged view of the Fourth Amendment could hardly be ignored, for [i]t follows from . . . *Silverman* . . . that the Fourth Amendment may protect against the overhearing of verbal statements as well as against the more traditional seizure of papers and effects," *Wong Sun v. United States*, 371 U.S. 471, 485 (1963).

Soon thereafter the Court repudiated the notion that the Fourth Amendment's protection was contingent upon some trespass to real property, *Katz v. United States*, 389 U.S. 347 (1967). Katz was a bookie convicted on the basis of evidence gathered by an electronic listening and recording device set up outside the public telephone booth that Katz used to take and place bets. The Court held that the gateway for Fourth Amendment purposes stood at that point where an individual should to able to expect that his or her privacy would not be subjected to unwarranted governmental intrusion, 389 U.S. at 353.[13]

One obvious consequence of Fourth Amendment coverage of wiretapping and other forms of electronic eavesdropping is the usual attachment of the Amendment's warrant requirement. To avoid constitutional problems and at the same time preserve wiretapping and other forms of electronic eavesdropping as a law enforcement tool, some of the states established a statutory system under which law enforcement officials could obtain a warrant, or equivalent court order, authorizing wiretapping or electronic eavesdropping.

The Court rejected the constitutional adequacy of one of the more detailed of these state statutory schemes in *Berger v. New York*, 388 U.S. 41 (1967). The statute was found deficient its failure to require:

- a particularized description of the place to be searched;
- a particularized description of the crime to which the search and seizure related;
- a particularized description of the conversation to be seized;

510-12 (internal quotation marks omitted).

[13] "We conclude that the underpinnings of *Olmstead* and *Goldman* have been so eroded by our subsequent decisions that the trespass doctrine there enunciated can no longer be regarded as controlling. The Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a search and seizure within the meaning of the Fourth Amendment. The fact that the electronic device employed to achieve that end did not happen to penetrate the wall of the booth can have no constitutional significance." Later courts seem to prefer the "expectation of privacy" language found in Justice Harlan's concurrence: "My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as reasonable," 389 U.S. at 361

- limitations to prevent general searches;
- termination of the interception when the conversation sought had been seized;
- prompt execution of the order;
- return to the issuing court detailing the items seized; and
- any showing exigent circumstances to overcome the want of prior notice. 388 U.S. at 58-60.

Berger help persuade Congress to enact Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 87 Stat. 197, 18 U.S.C. 2510 - 2520 (1970 ed.), a comprehensive wiretapping and electronic eavesdropping statute that not only outlawed both in general terms but that permitted federal and state law enforcement officers to use them under strict limitations designed to meet the objections in *Berger*.

A decade later another Supreme Court case persuaded Congress to supplement Title III with a judicially supervised procedure for the use of wiretapping and electronic eavesdropping in foreign intelligence gathering situations.

When Congress passed Title III there was some question over the extent of the President's inherent powers to authorize wiretaps – without judicial approval – in national security cases. As a consequence, the issue was simply removed from the Title III scheme.[14] After the Court held that the President's inherent powers were insufficient to excuse warrantless electronic eavesdropping on purely domestic threats to national security, *United States v. United States District Court*, 407 U.S. 297 (1972), Congress considered it prudent to augment the foreign intelligence gathering authority of the United States with the Foreign Intelligence Security Act of 1978, 92 Stat. 1783, 50 U.S.C. 1801 - 1811. The Act provides a procedure for judicial review and authorization or denial of wiretapping and other forms of electronic eavesdropping for purposes of foreign intelligence gathering.

In 1986, Congress recast Title III in the Electronic Communications Privacy Act (ECPA), 100 Stat. 1848, 18 U.S.C. 2510 - 2521. The Act followed the general outline of Title III with adjustments and additions. Like Title III, it sought to strike a balance between the interests of privacy and law enforcement, but it also reflected a Congressional desire to avoid unnecessarily crippling infant industries in the fields of advanced communications technology, H.R.Rep.No. 647, 99th Cong., 2d Sess. 18-9 (1984); S.Rep.No. 541, 99th Cong., 2d Sess. 5 (1986).

The Act also included new protection and law enforcement access provisions for stored wire and electronic communications and transactional records access (e-mail and phone records), 18 U.S.C. 2701 - 2710, and for pen registers as well as trap and trace devices (devices for recording the calls placed to or from a particular telephone), 18 U.S.C. 3121 - 3126.

---

[14] 18 U.S.C. 2511(3)(1970 ed.)("Nothing contained in this chapter or in section 605 of the Communications Act . . . shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities. . .").

Over the years, Congress has adjusted the components of Title III/ECPA or FISA. Sometimes in the interests of greater privacy; sometimes in the interest of more effective law enforcement or foreign intelligence gathering. The 107th Congress, for instance, amended the basic statutes in the USA PATRIOT Act, P.L. 107-56, 115 Stat. (2001); the Intelligence Authorization Act for Fiscal Year 2002, P.L. 107-108, 115 Stat. 1394 (2001); the 21st Century Department of Justice Appropriations Authorization Act, P.L. 107-273, 116 Stat. 1758 (2002); and the Department of Homeland Security Act, P.L. 107-296, 116 Stat. 2135 (2002).

Prohibitions

Generally

Unless otherwise provide, Title III/ECPA outlaws wiretapping and other forms of electronic eavesdropping, possession of wiretapping or electronic eavesdropping equipment, use or disclosure of information obtained through illegal wiretapping or electronic eavesdropping, and in order to obstruct justice, disclosure of information secured through court-ordered wiretapping or electronic eavesdropping, 18 U.S.C. 2511. There are separate crimes for:

- unlawful access to stored communications, 18 U.S.C. 2701;
- unlawful use of a pen register or a trap and trace device, 18 U.S.C. 3121; and
- abuse of eavesdropping authority or unlawful disclosures under the Foreign Intelligence Surveillance Act, 50 U.S.C. 1809, 1827.

Illegal Wiretapping and Electronic Eavesdropping

At the heart of Title III/ECPA lies the prohibition against illegal wiretapping and electronic eavesdropping, 18 U.S.C. 2511(1), that proscribes:

- any person from
- intentionally
- intercepting, or endeavoring to intercept, or
- wire, oral or electronic communications
- by using an electronic, mechanical or other device
- unless the conduct is specifically authorized or expressly not covered, *e.g.*
  - one of the parties to the conversation has consent to the interception
  - the interception occurs in compliance with a statutorily authorized, (and ordinarily judicially-supervised) law enforcement or foreign intelligence gathering interception,
  - the interception occurs as part of providing or regulating communication services,
  - certain radio broadcasts, and
  - in some places, spousal wiretappers.

Person

The prohibition applies to "any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation," 18 U.S.C. 2510(6).[15]

Intentional

Conduct can only violate Title III/ECPA if it is done "intentionally," inadvertent conduct is no crime; the offender must have done on purpose those things which are outlawed.[16]

Jurisdiction

Section 2511(1) contains two interception bars – one, 2511(1)(a), simply outlaws intentional interception; the other, 2511(1)(b), outlaws intentional interception when committed under any of five jurisdictional circumstances.[17] Congress adopted the approach because of concern that its constitutional authority might not be sufficient to ban instances of electronic surveillance that bore no discernable connection to interstate commerce or any other of the enumerated powers. So it enacted a general prohibition, and as a safety precaution, a second provision more tightly tethered to specific jurisdictional factors.[18] The Justice

---

[15] Although the governmental entities are not subject to criminal liability, as noted *infra*, the some courts believe them subject to civil liability under 18 U.S.C. 2520.

[16] "In order to underscore that the inadvertent reception of a protected communication is not a crime, the subcommittee changed the state of mind requirement under Title III of the Omnibus Crime Control and Safe Streets Act of 1968 from 'willful' to 'intentional,'" S.REP.NO. 541, 99th Cong., 2d Sess. 23 (1986); "This provision makes clear that the inadvertent interception of a protected communication is not unlawful under this Act," H.REP.NO. 647, 99th Cong., 2d Sess. 48-9 (1986).

[17] "(1) Except as otherwise specifically provided in this chapter any person who – (a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;

"(b) intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when – (i) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or "(ii) such device transmits communications by radio, or interferes with the transmission of such communication; or (iii) such person knows, or has reason to know, that such device or any component thereof has been sent through the mail or transported in interstate or foreign commerce; or (iv) such use or endeavor to use (A) takes place on the premises of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or (B) obtains or is for the purpose of obtaining information relating to the operations of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or (v) such person acts in the District of Columbia, the Commonwealth of Puerto Rico, or any territory or possession of the United States," 18 U.S.C. 2511(1)(a),(b).

[18] "Subparagraph (a) establishes a blanket prohibition against the interception of wire communication. Since the facilities used to transmit wire communications form part of the interstate or foreign communications network, Congress has plenary power under the commerce clause to prohibit all interception of such communications whether by wiretapping or otherwise.

Department has honored that caution by employing subparagraph (b) to prosecute the interception of oral communications, while using subparagraph (a) to prosecute other forms of electronic eavesdropping, DEPARTMENT OF JUSTICE CRIMINAL RESOURCE MANUAL at 1050.

Interception

Interception "means the aural or other acquisition of the contents" of various kinds of communications.[19] ECPA enlarged the definition by adding the words "or other acquisition" so that it is no longer limited to interceptions that can be heard.[20]

Endeavoring to intercept

Although the statute condemns attempted wiretapping and electronic eavesdropping ("endeavoring to intercept"), 18 U.S.C. 2511(1), the provisions appear to have escaped use, interest, or comment heretofore, perhaps because the conduct most likely to constitute preparation for an interception – possession of wiretapping equipment – is already a separate crime, 18 U.S.C. 2512, discussed, *infra*.

"The broad prohibition of subparagraph (a) is also applicable to the interception of oral communications. The interception of such communications, however, does not necessarily interfere with the interstate or foreign commerce network, and the extent of the constitutional power of Congress to prohibit such interception is less clear than in the case of interception of wire communications. . . .

"Therefore, in addition to the broad prohibitions of subparagraph (a), the committee has included subparagraph (b), which relies on accepted jurisdictional bases under the commerce clause, and other provisions of the Constitution to prohibit the interception of oral communications," S.REP.NO.1097, 90th Cong., 2d Sess. 91-2 (1968).

[19] The dictionary definition of "aural" is "of or relating to the ear or to the sense of hearing," MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY 76 (10th ed. 1996).

[20] S.Rep.No. 541, 99th Cong., 2d Sess. 13 (1986)(the "amendment clarifies that it is illegal to intercept the non-voice portion of a wire communication. For example, it is illegal to intercept the data or digitized portion of a voice communication"); *see also* H.REP.NO. 647, 99th Cong., 2d Sess. 34 (1986).

By electronic, mechanical, or other device

The statute does not cover common law "eavesdropping," but only interceptions "by electronic, mechanical or other device," 18 U.S.C. 2510(4). That phrase is in turn defined so as not to include hearing aids or extension telephones in normal use.[21] Whether an extension phone has been installed and is being used in the ordinary course of business or in the ordinary course of law enforcement duties, so that it no longer constitutes an interception device for purposes of Title III/ECPA and comparable state laws has proven a somewhat vexing question.[22]

Although often intertwined with the consent exception discussed below, the question generally turns on the facts in a given case.[23] When the exemption is claimed as a practice in the ordinary course of business, the interception must be for a legitimate business reason, it must be routinely conducted, and at least in some circuits employees must be notified at that their conversations are being monitored.[24] Similarly, "Congress most likely carved out an exception for law enforcement officials to make clear that the routine and almost universal recording of phone lines by police departments and prisons, as well as other law enforcement institutions, is exempt from the statute," *Adams v. Battle Creek*, 250 F.3d at 984.[25] The exception

---

[21] "'[E]lectronic, mechanical, or other device' means any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than – (a) any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business; or (ii) being used by a provider of wire or electronic communication service in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties; (b) a hearing aid or similar device being used to correct subnormal hearing to not better than normal," 18 U.S.C. 2510(5).

[22] See the cases cited and commentary in Barnett & Makar, *"In the Ordinary Course of Business": The Legal Limits of Workplace Wiretapping*, 10 HASTINGS JOURNAL OF COMMUNICATIONS AND ENTERTAINMENT LAW 715 (1988); *Application to Extension Telephones of Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (18 U.S.C. §§2510 et seq.), Pertaining to Interceptions of Wire Communications*, 58 ALR Fed. 594; *Eavesdropping on Extension Telephone as Invasion of Privacy*, 49 ALR 4th 430.

[23] *See e.g., Deal v. Spears*, 780 F.Supp. 618, 623 (W.D.Ark. 1991), *aff'd*, 980 F.2d 1153 (8th Cir. 1992)(employer regularly taped employee calls by means of a device attached to an extension phone; most of the calls were personal and recording and disclosing them served no business purpose).

[24] *Adams v. Battle Creek*, 250 F.3d 980, 983 (6th Cir. 2001); *Arias v. Mutual Central Alarm Service*, 202 F.3d 553, 558 (2d Cir. 2000); *Berry v. Funk*, 146 F.3d 1003, 1008 (D.C.Cir. 1998); *Sanders v. Robert Bosch Corp.*, 38 F.3d 736, 741 (4th Cir. 1994).

Some courts include surreptitious, extension phone interceptions conducted within the family home as part of the "business extension" exception, *Anonymous v. Anonymous*, 558 F.2d 677, 678-79 (2d Cir. 1977); *Scheib v. Grant*, 22 F.3d 149, 154 (7th Cir. 1994); *Newcomb v. Ingle*, 944 F.2d 1534, 1536 (10th Cir. 1991); *contra, United States v. Murdock*, 63 F.3d 1391, 1400 (6th Cir. 1995).

[25] *See e.g., Smith v. U.S.Dept. of Justice*, 251 F.3d 1647, 1049-50 (D.C.Cir. 2001); *United States v. Poyck*, 77 F.3d 285, 292 (9th Cir. 1996); *United States v. Daniels*, 902 F.2d 1238,

contemplates administrative rather than investigative monitoring,[26] which must nevertheless be justified by a lawful, valid law enforcement concern.[27]

Wire, oral or electronic communications

An interception can only be a violation of ECPA if the conversation or other form of communication intercepted is among those kinds which the statute protects, in over simplified terms – telephone (wire), face to face (oral), and computer (electronic). Congress used the definitions of the three forms of communications to describe the communications beyond the Act's reach as well as those within its grasp. For example, "oral communication" by definition includes only those face to face conversations with respect to which the speakers have a justifiable expectation of privacy.[28] Similarly, "wire communications" are limited to those that are at some point involve voice communications (i.e. only aural transfers). [29] Radio and data

---

1245 (7th Cir. 1990); *United States v. Paul*, 614 F.2d 115, 117 (6th Cir. 1980).

[26] *Amati v. Woodstock*, 176 F.3d 952, 955 (7th Cir. 1999)("Investigation is within the ordinary course of law enforcement, so if 'ordinary' were read literally warrants would rarely if ever be required for electronic eavesdropping, which was surely not Congress's intent. Since the purpose of the statute was primarily to regulate the use of wiretapping and other electronic surveillance for investigatory purposes, 'ordinary' should not be read so broadly; it is more reasonably interpreted to refer to routine noninvestigative recording of telephone conversations").

[27] The exception, however, does not permit a county to record all calls in and out of the offices of county judges merely because a detention center and the judges share a common facility, *Abraham v. Greenville*, 237 F.3d 386, 390 (4th Cir. 2001), nor does it permit jailhouse telephone monitoring of an inmate's confession to a clergyman, *Mockaitis v. Harcleroad*, 104 F.3d 1522, 1530 (9th Cir. 1997).

[28] "'[O]ral communication' means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication," 2510(2). Unlike the definitions of wire and electronic communications, infra, there is no reference to interstate or foreign commerce here, see, *United States v. Duncan*, 598 F.2d 839, 854 (4th Cir. 1979)(upholding a conviction for interception of an oral communication on the grounds that the question of whether an activity has an impact on interstate commerce is a question for Congress; the Supreme Court subsequent established a more demanding standard the exercise of Congress' commerce clause powers in *United States v. Lopez*, 514 U.S. 549 (1995) and *United States v. Morrison*, 529 U.S. 598 (2000)); *United States v. Carnes*, 309 F.3d 950, 954 (7th Cir. 2002)(rejecting constitutional challenge to a conviction under 18 U.S.C. 2511 with the observation that the wire communication definition specifically referred to interstate and foreign commerce). The potential problem is addressed, however, in paragraph 2511(1)(b) where the ban on illicit capture of oral communications is tied to elements of interstate commerce, supra at 8-9.

[29] "'[W]ire communication' means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce ~~and such term includes any electronic storage of such communication~~," 18 U.S.C. 2510(1)(The USA PATRIOT Act struck the language noted above in order to remove stored voice mail from

transmissions are generally "electronic communications." The definition includes other forms of information transfer but excludes certain radio transmissions which can be innocently captured without great difficulty.[30] Although it is not a federal crime to intercept radio communications under any number of conditions, the exclusion is not a matter of definition but of special general exemptions, 18 U.S.C. 2511(2)(g), discussed below.

Exemptions: consent interceptions

Consent interceptions are common, controversial and have a history all their own. The early bans on divulging telegraph or telephone messages had a consent exception The Supreme Court upheld consent interceptions against Fourth Amendment challenge both before and after the enactment of Title III.[31] The argument in favor of consent interceptions has always been essentially that a speaker risks the indiscretion of his listeners and holds no superior legal position simply because a listener elects to record or transmit his statements rather than subsequently memorializing or repeating them.[32] Wiretapping or electronic eavesdropping by

---

the coverage of Title III, 115 Stat. 283 (2001); the definition reverts to its original form when the USA PATRIOT Act amendment sunsets on Dec. 31, 2005).

[30] "'[E]lectronic communication' means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include – (A) the radio portion of a cordless telephone communication that is transmitted between the cordless handset and the base unit; (B) any wire or oral communication; (C) any communication made through a tone-only paging device; or (D) any communication from a tracking device (as defined in section 3117 of this title)," 18 U.S.C. 2510(12).

[31] *On Lee v. United States*, 343 U.S. 747 (1952); *Lopez v. United States*, 373 U.S. 427 (1963); *United States v. White*, 401 U.S. 745 (1971).

[32] *United States v. White*, 401 U.S. at 751 (1971)("Concededly a police agent who conceals his police connections may write down for official use his conversations with a defendant and testify concerning them, without a warrant authorizing his encounters with the defendant and without otherwise violating the latter's Fourth Amendment rights . . . . For constitutional purposes, no different result is required if the agent instead of immediately reporting and transcribing his conversations with defendant, either (1) simultaneously records them with electronic equipment which he is carrying on his person, *Lopez v. United States, supra*; (2) or carries radio equipment which simultaneously transmits the conversations either to recording equipment located elsewhere or to other agents monitoring the transmitting frequency. *On Lee v. United States, supra.* If the conduct and revelations of an agent operating without electronic equipment do not invade the defendant's constitutionally justifiable expectations of privacy, neither does a simultaneous recording of the same conversations made by the agent or by others from transmissions received from the agent to whom the defendant is talking and whose trustworthiness the defendant necessarily risks"); *Lopez v. United States* 373 U.S. 427, 439 (1963)("Stripped to its essentials, petitioner's argument amounts to saying that he has a constitutional right to rely on possible flaws in the agent's memory, or to challenge the agent's credibility without being beset by corroborating evidence that is not susceptible of impeachment. For no other argument can justify excluding an accurate version of a conversation that the agent could testify to from memory. We think the risk that petitioner took in offering a bribe to Davis fairly included the risk that the offer would be accurately reproduced in court, whether by faultless memory or

either the police or anyone else with the consent of at least one party to the conversation is not unlawful under the federal statute.[33] These provisions do no more than shield consent interceptions from the sanctions of federal law; they afford no protection from the sanctions of state law. Many of the states recognize comparable exceptions, but some only permit interception with the consent of *all* parties to a communication.[34]

Under federal law, consent may be either explicitly or implicitly given. For instance, someone who uses a telephone other than his or her own and has been told by the subscriber that conversations over the instrument are recorded has been held to have implicitly consented to interception when using the instrument.[35] This is not to say that subscriber consent alone is sufficient, for it is the parties to the conversation whose privacy is designed to protect.[36] Although consent may be given in the hopes of leniency from law enforcement officials or as an election between unpalatable alternatives, it must be freely given and not secured coercively.[37]

Private consent interceptions may not be conducted for a criminal or tortious purpose. At one time, the limitation encompassed interceptions for criminal, tortious, *or* otherwise injurious purposes, but ECPA dropped the reference to injurious purposes for fear that first amendment values might be threatened should the clause be read to outlaw consent interceptions conducted to embarrass, S.REP.NO. 541, 99th Cong., 2d Sess. 17-8 (1986); H.REP.NO. 647, 99th Cong., 2d Sess. 39-40 (1986).

Exemptions: publicly accessible radio communications

---

mechanical recording").

[33] "(c) It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception.

"(d) It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State," 18 U.S.C. 2511(2)(c),(d).

[34] For citations to state law see Appendix II.

[35] *United States v. Footman*, 215 F.3d 145, 154-55 (1st Cir. 2000) (inmate use of prison phone); *Griggs-Ryan v. Smith*, 904 F.2d 112, 116-17 (1st Cir. 1990)(use of landlady's phone).

[36] *Anthony v. United States*, 667 F.2d 870, 876 (10th Cir. 1981).

[37] *United States v. Antoon*, 933 F.2d 200, 203-204 (3d Cir. 1991), but see, *O'Ferrell v. United States*, 968 F.Supp. 1519, 1541 (M.D.Ala. 1997)(an individual – who spoke to his wife on the telephone after being told by FBI agents, then executing a search warrant at his place of business, that he could only speak to her with the agents listening in – consented to the interception, even if FBI's initial search were unconstitutional).

Radio communications which can be inadvertently heard or are intended to be heard by the public are likewise exempt. These include not only commercial broadcasts, but ship and aircraft distress signals, tone-only pagers, marine radio and citizen band radio transmissions, and interceptions necessary to identify the source any transmission, radio or otherwise, disrupting communications satellite broadcasts.[38]

Exemptions: government officials

Government officials enjoy an exemption when acting under judicial authority, whether that provided in Title III/ECPA for federal and state law enforcement officers,[39] the Foreign Intelligence Surveillance Act,[40] or the separate provisions according them access to stored electronic communications and the use of pen registers and trap and trace devices.[41]

Exemptions: communication service providers

---

[38] "(g) It shall not be unlawful under this chapter or chapter 121 of this title for any person – (i) to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public;

"(ii) to intercept any radio communication which is transmitted – (I) by any station for the use of the general public, or that relates to ships, aircraft, vehicles, or persons in distress; (II) by any governmental, law enforcement, civil defense, private land mobile, or public safety communications system, including police and fire, readily accessible to the general public; (III) by a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services; or (IV) by any marine or aeronautical communications system;

"(iii) to engage in any conduct which – (I) is prohibited by section 633 of the Communications Act of 1934; or (II) is excepted from the application of section 705(a) of the Communications Act of 1934 by section 705(b) of that Act;

"(iv) to intercept any wire or electronic communication the transmission of which is causing harmful interference to any lawfully operating station or consumer electronic equipment, to the extent necessary to identify the source of such interference; or

"(v) for other users of the same frequency to intercept any radio communication made through a system that utilizes frequencies monitored by individuals engaged in the provision or the use of such system, if such communication is not scrambled or encrypted," 18 U.S.C. 2511(2)(g).

[39] "*Except as otherwise specifically provided in this chapter* any person who (a) intentionally intercepts . . . ." 18 U.S.C. 2511(1)(emphasis added).

[40] "(e) Notwithstanding any other provision of this title or section 705 or 706 of the Communications Act of 1934, it shall not be unlawful for an officer, employee, or agent of the United States in the normal course of his official duty to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, as authorized by that Act,"18 U.S.C. 2511(2)(e).

[41] "(h) It shall not be unlawful under this chapter – (i) to use a pen register or a trap and trace device (as those terms are defined for the purpose of chapter 206). . . ." 18 U.S.C. 2511(2)(h). For the citations to state statutes permitting judicial authorization of law enforcement interception of wire, oral or electronic communications, for access to stored electronic communications, and for the use pen registers and trap and trace devices see Appendix V.

There is a general exemption for those associated with supplying communications services, the telephone company, switchboard operators, and the like. The exemption not only permits improved service and lets the telephone company protect itself against fraud,[42] but it allows for assistance to federal and state officials operating under a judicially supervised interception order,[43] and for the

---

[42] "(a)(i) It shall not be unlawful under this chapter for an operator of a switchboard, or on officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks . . .

* * *

"(h) It shall not be unlawful under this chapter . . .

"(ii) for a provider of electronic communication service to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire or electronic communication, or a user of that service, from fraudulent, unlawful or abusive use of such service," 18 U.S.C. 2511(2)(a)(i),(h).

[43] "(ii) Notwithstanding any other law, providers of wire or electronic communication service, their officers, employees, and agents, landlords, custodians, or other persons, are authorized to provide information, facilities, or technical assistance to persons authorized by law to intercept wire, oral, or electronic communications or to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, if such provider, its officers, employees, or agents, landlord, custodian, or other specified person, has been provided with –

(A) a court order directing such assistance signed by the authorizing judge, or

(B) a certification in writing by a person specified in section 2518(7) of this title or the Attorney General of the United States that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required,

setting forth the period of time during which the provision of the information, facilities, or technical assistance is authorized and specifying the information, facilities, or technical assistance required. No provider of wire or electronic communication service, officer, employee, or agent thereof, or landlord, custodian, or other specified person shall disclose the existence of any interception or surveillance or the device used to accomplish the interception or surveillance with respect to which the person has been furnished a court order or certification under this chapter, except as may otherwise be required by legal process and then only after prior notification to the Attorney General or to the principal prosecuting attorney of a State or any political subdivision of a State, as may be appropriate. Any such disclosure, shall render such person liable for the civil damages provided for in section 2520. No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, or agents, landlord, custodian, or other specified person for providing information, facilities, or assistance in accordance with the terms of a court order, *statutory authorization,* or certification under this chapter," 18 U.S.C. 2511(2)(a)(ii). The Homeland Security Act, 116 Stat. 2158 (2002), added the language in italics to "ensure that providers of communications remain covered under 18 U.S.C. 2511(a)(a)(ii), another 'no cause of action' provision which protects providers from law suits when they are legally assisting law enforcement with an investigation under the new computer trespasser provision, §2511(2)(i), created in the USA PATRIOT Act," H.Rep.No. 107-497 at 16 (2002).

regulatory activities of the Federal Communications Commission.[44]

Domestic exemptions

A few courts recognize a "vicarious consent" exception under which a custodial parent may secretly record the conversations of his or her minor child in the interest of protecting the child.[45] Although rejected by most,[46] a handful of federal courts have held that Title III/ECPA does not preclude one spouse from wiretapping or electronically eavesdropping upon the other,[47] a result other courts have sometimes reached through the telephone extension exception discussed above.[48]

Subject to the same exceptions, section 2511 also protects wire, oral and electronic communications from any person who intentionally:

- discloses or endeavors to disclose information with reason to know it has been unlawfully intercepted, or
- uses or endeavors to use information with reason to know it has been unlawfully intercepted, or
- discloses or endeavors to disclose information with intent to obstruct justice and with reason to know the information was secured through a court-ordered interception.

---

[44] "(b) It shall not be unlawful under this chapter for an officer, employee, or agent of the Federal Communications Commission, in the normal course of his employment and in discharge of the monitoring responsibilities exercised by the Commission in the enforcement of chapter 5 of title 47 of the United States Code, to intercept a wire or electronic communication, or oral communication transmitted by radio, or to disclose or use the information thereby obtained," 18 U.S.C. 2511(2)(b).

[45] *Pollock v. Pollock*, 154 F.3d 601, 611 (8th Cir. 1998); *Wagner v. Wagner*, 64 F.Supp.2d 895, 889-901 (D.Minn. 1999); *Campbell v. Price*, 2 F.Supp.2d 1186, 1191-192 (E.D.Ark. 1998); *Thompson v. Dulaney*, 838 F.Supp. 1535 (D.Utah 1993).

[46] *Heggy v. Heggy*, 944 F.2d 1537, 1539 (10th Cir. 1991); *Kempf v. Kempf*, 868 F.2d 970, 972 (8th Cir. 1989); *Pritchard v. Pritchard*, 732 F.2d 372, 374 (4th Cir. 1984); *United States v. Jones*, 542 F.2d 661, 667 (6th Cir. 1976); *Kratz v. Kratz*, 477 F.Supp. 463, 467-70 (E.D.Pa. 1979); *Heyman v.Heyman*, 548 F.Supp. 1041, 1045-47 (N.D.Ill.1982); *Lombardo v. Lombardo*, 192 F.Supp.2d 885, 809 (N.D.Ill. 2002).

[47] *Simpson v. Simpson*, 490 F.2d 803, 809 (5th Cir. 1974); *Perfit v. Perfit*, 693 F.Supp. 854-56 (C.D.Cal. 1988); see generally, *Applicability, in Civil Action, of Provisions of Omnibus Crime Control and Safe Streets Act of 1968 Prohibiting Interception of Communications (18 USCS §2511(1)), to Interception by Spouse, or Spouse's Agent, of Conversations of Other Spouse*, 139 ALR FED. 517, and the cases discussed therein.

[48] *Anonymous v. Anonymous*, 558 F.2d 677, 678-79 (2d Cir. 1977); *Scheib v. Grant*, 22 F.3d 149, 154 (7th Cir. 1994); *Newcomb v. Ingle*, 944 F.2d 1534, 1536 (10th Cir. 1991); *contra, United States v. Murdock*, 63 F.3d 1391, 1400 (6th Cir. 1995).

Consequences: Criminal Penalties

Interceptions in violation of Title III/ECPA are generally punishable by imprisonment for not more than five years and/or a fine of not more than $250,000 for individuals and not more than $500,000 for organizations.[49] The same penalties apply to the unlawful capture of cell phone and cordless phone conversations, now that the Homeland Security Act, 116 Stat. 2158 (2002), has repealed the reduced penalty provisions that at one time applied to the unlawful interceptions using radio scanners and the like, 18 U.S.C. 2511(4)(b)(2000 ed.). There is a reduced penalty, however, for filching satellite communications as long as the interception is not conducted for criminal, tortious, nor mercenary purposes, is the second instance where Congress opted for reduced penalties. Unauthorized interception is broadly proscribed subject to an exception for unscrambled transmissions,[50] are subject to the general 5-year penalty, but interceptions for neither criminal, tortious, nor mercenary purposes, subject offenders to only civil punishment.[51] Equipment used

---

[49] "Except as provided in (b) of this subsection or in subsection (5), whoever violates subsection (1) of this section shall be fined under this title* or imprisoned not more than five years, or both." 18 U.S.C. 2511(4)(a).

* Section 3559 of title 18 classifies as a felony any offense punishable by imprisonment for more than one year; and as a class A misdemeanor any offense punishable by imprisonment for one year or less but not more than six months. Unless Congress clearly rejects the general fine ceilings it provides, section 3571 of title 18 sets the fines for felonies at not more than $250,000 for individuals and not more than $500,000 for organizations, and for class A misdemeanors at not more than $100,000 for individuals and not more than $200,000 for organizations. If there is monetary loss or gain associated with the offense, the offender may alternatively be fined not more than twice the amount of the loss or gain, 18 U.S.C. 3571.

[50] "(b) Conduct otherwise an offense under this subsection that consists of or relates to the interception of a satellite transmission that is not encrypted or scrambled and that is transmitted – (i) to a broadcasting station for purposes of retransmission to the general public; or (ii) as an audio subcarrier intended for redistribution to facilities open to the public, but not including data transmissions or telephone calls, is not an offense under this subsection unless the conduct is for the purpose of direct or indirect commercial advantage or private financial gain," 18 U.S.C. 2511(4)(b).

[51] "(5)(a)(i) If the communication is – (A) a private satellite video communication that is not scrambled or encrypted and the conduct in violation of this chapter is the private viewing of that communication and is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain; or (B) a radio communication that is transmitted on frequencies allocated under subpart D of part 74 of the rules of the Federal Communications Commission that is not scrambled or encrypted and the conduct in violation of this chapter is not for tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, then the person who engages in such conduct shall be subject to suit by the Federal Government in a court of competent jurisdiction. (ii) In an action under this subsection – (A) if the violation of this chapter is a first offense for the person under paragraph (a) of subsection (4) and such person has not been found liable in a civil action under section 2520 of this title, the Federal Government shall be entitled to appropriate injunctive relief; and (B) if the violation of this chapter is a second or subsequent offense under paragraph (a) of subsection (4) or such person has been found liable in any prior civil action under section 2520, the person shall be subject to a mandatory $500 civil fine.

"(b) The court may use any means within its authority to enforce an injunction issued

to wiretap or eavesdrop in violation of Title III is subject to confiscation by the United States, either in a separate civil proceeding or a part of the prosecution of the offender.[52]

In addition to exemptions previously mentioned, Title III provides a defense to criminal liability based on good faith.[53] As noted below, the defense seems to lack

---

under paragraph (ii)(A), and shall impose a civil fine of not less than $500 for each violation of such an injunction." 18 U.S.C. 2511(5).

Under 18 U.S.C. 2520, victims may recover no more than damages of not less than $50 nor more than $500 for the first offense, increased to $100 and $1000 for subsequent offenses.

[52] 18 U.S.C. 2513 ("Any electronic, mechanical, or other device used, sent, carried, manufactured, assembled, possessed, sold, or advertised in violation of section 2511 or section 2512 of this chapter may be seized and forfeited to the United States. . ."); 18 U.S.C. 983(a)(3)(C)("In lieu of, or in addition to, filing a civil forfeiture complaint, the Government may include a forfeiture allegation in a criminal indictment. . .").

[53] "A good faith reliance on – (1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization; (2) a request of an investigative or law enforcement officer under section 2518(7) of this title; or (3) a good faith determination that section 2511(3)* *or 2511(2)(i)*** of this title permitted the conduct complained of; is a complete defense against any civil or criminal action brought under this chapter or any other law," 18 U.S.C. 2520(d). The Homeland Security Act added the language in italics above, 116 Stat. 2157 (2002), which was thought to provide a defense to civil liability for good faith providers who assisted law enforcement officials in the interception of computer trespasser communications within the provider's system, H.Rep.No.107-497 at 14-5 (2002). On its face, the language appears to provide a good faith defense to intercepting officers in a trespass situation.

*"(3)(a) Except as provided in paragraph (b) of this subsection, a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.

"(b) A person or entity providing electronic communication service to the public may divulge the contents of any such communication – (i) as otherwise authorized in section 2511(2)(a) or 2517 of this title; (ii) with the lawful consent of the originator or any addressee or intended recipient of such communication; (iii) to a person employed or authorized, or whose facilities are used, to forward such communication to its destination; or (iv) which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency," 18 U.S.C. 2511(3).

**"*(i) It shall not be unlawful under this chapter for a person acting under color of law to intercept the wire or electronic communications of a computer trespasser transmitted to, through, or from the protected computer if (I) the owner or operator of the protected computer authorizes the interception of the computer trespasser's communications on the protected computer; (II) the person acting under color of law is lawfully engaged in an investigation; (III) the person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser's communications will be relevant to the investigation; and (IV) such interception does not acquire communications other than those transmitted to or from the computer trespasser*," 18 U.S.C. 2511(2)(i). This language was added by the USA PATRIOT Act, 115 Stat. 291 (2001); it expires when the USA PATRIOT Act amendment sunsets on Dec. 31, 2005, 115 Stat. 295 (2001). A "protected computer" is

sufficient breadth to shelter any offender other than a government official or some one working at their direction.

Consequences: Civil Liability

Victims of illegal wiretapping or electronic eavesdropping may be entitled equitable relief, damages (equal to the greater of actual damages, $100 per day of violation, or $10,000),[54] punitive damages, reasonable attorney's fees and reasonable litigation costs, 18 U.S.C. 2520.[55] There is a division of authority as to whether (1) a court may decline to award damages, attorneys' fees and costs once a violation has been

---

"a computer – (A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or (B) which is used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States," 18 U.S.C. 1030(e)(2).

[54] The $10,000 lump sum for liquidated damages is limited to a single award per victim rather than permitting $10,000 multiples based on the number of violations or the number of types of violations, as long as the violations are "interrelated and time compacted," *Smoot v. United Transportation Union*, 246 F.3d 633, 642-645 (6th Cir. 2001); *Desilets v. Wal-Mart Stores, Inc.*, 171 F.3d 711, 713 (1st Cir. 1999).

[55] "(a) Except as provided in section 2511(2)(a)(ii), any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity, *other than the United States*, which engaged in that violation such relief as may be appropriate.

"(b) In an action under this section, appropriate relief includes – (1) such preliminary and other equitable or declaratory relief as may be appropriate; (2) damages under subsection (c) and punitive damages in appropriate cases; and (3) a reasonable attorney's fee and other litigation costs reasonably incurred.

"(c) (1) [relating to satellite video]. (2) In any other action under this section, the court may assess as damages whichever is the greater of – (A) the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation; or (B) statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000.

"(d) A good faith reliance on – (1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization; (2) a request of an investigative or law enforcement officer under section 2518(7) of this title; or (3) a good faith determination that section 2511(3) *or 2511(2)(i)* of this title permitted the conduct complained of; is a complete defense against any civil or criminal action brought under this chapter or any other law.

"(e) A civil action under this section may not be commenced later than two years after the date upon which the claimant first has a reasonable opportunity to discover the violation.

(f) [Administrative discipline]

"(g) Any willful disclosure or use by an investigative or law enforcement officer or governmental entity of information beyond the extent permitted by section 2517 is a violation of this chapter for purposes of section 2520(a)," 18 U.S.C. 2520. The USA PATRIOT Act established separate provisions to cover civil actions against the United States, 115 Stat. 293-94 (2001), discussed below, and consequently explicitly excluded suits against the United States from section 2520. Both the separate provisions and the changes in 18 U.S.C. 2520 expire when the USA PATRIOT Act amendments sunset on December 31, 2005, 115 Stat. 295 (2001).

shown,[56] (2) governmental entities other than the United States are liable for violations of section 2520,[57] and (3) law enforcement officers enjoy a qualified immunity from suit under section 2520.[58]

The cause of action created in section 2520 is subject to a good faith defense, 18 U.S.C. 2520(d). The only apparent efforts to claim the defense by any one other than a government official or someone working at their direction have been unsuccessful.[59]

Consequences: Civil Liability of the United States

The USA PATRIOT Act authorizes a cause of action against the United States for willful violations of Title III, the Foreign Intelligence Surveillance Act or the provisions governing stored communications in 18 U.S.C. 2701-2712, 18 U.S.C. 2712.[60]

---

[56] *Compare*, *Nalley v. Nalley*, 53 F.3d 649, 651-53 (4th Cir. 1995), *Reynolds v. Spears*, 93 F.3d 428, 433 (8th Cir. 1996); *Romano v. Terkik*, 939 F.Supp. 144, 146-47 (D.Conn. 1996)(courts have discretion), *with*, *Rodgers v. Wood*, 910 F.2d 444, 447-49 (7th Cir. 1990) and *Menda Biton v. Menda*, 812 F.Supp. 283, 284 (D. Puerto Rico 1993)(courts have no such discretion)(note that after *Menda*, the First Circuit in *Desilets v. Wal-Mart Stores, Inc.*, 171 F.3d at 716-17 treated as a matter for the trial court's discretion the question of whether the award of plaintiff's attorneys' fees should be reduced when punitive damages have been denied).

[57] *Adams v. Battle Creek*, 250 F.3d 980, 984 (6th Cir. 2001); *Organizacion JD Ltda. v. United States Department of Justice*, 18 F.3d 91, 94-5 (2d Cir. 1994); *Connor v. Tate*, 120 F.Supp.2d 1370, 1374 (N.D.Ga. 2001); *Dorris v. Absher*, 959 F.Supp. 813, 820 (M.D.Tenn. 1997), *aff'd/rev'd in part on other grounds*, 179 F.3d 420 (6th Cir. 1999); *PBA Local No. 38 v. Woodbridge Police Department*, 832 F.Supp. 808, 822-23 (D.N.J. 1993)(each concluding that governmental entities may be held liable); *contra*, *Abbott v. Winthrop Harbor*, 205 F.3d 976, 980 (7th Cir. 2000); *Amati v. Woodstock*, 176 F.3d 952, 956 (7th Cir. 1999).

[58] *Compare, Berry v. Funk*, 146 F.3d 1003, 1013 (D.C.Cir. 1998)(no immunity), *with, Tapley v. Collins*, 211 F.3d 1210, 1216 (11th Cir. 2000)(immunity); *Blake v. Wright*, 179 F.3d 1003, 1011-13(6th Cir. 1999)(same); see generally, *Qualified Immunity as Defense in Suit Under Federal Wiretap Act (18 U.S.C.A. §§2510 et seq.)*, 178 ALR FED. 1.

[59] *Williams v. Poulos*, 11 F.3d 271, 285 (1st Cir. 1993); *United States v. Wuliger*, 981 F.2d 1497, 1507 (6th Cir. 1992).

[60] "(a) Any person who is aggrieved by any willful violation of this chapter or of chapter 119 of this title or of sections 106(a), 305(a), or 405(a) of the Foreign Intelligence Surveillance Act of 1978 (50 U. S.C. 1801 et seq.) may commence an action in United States District Court against the United States to recover money damages. In any such action, if a person who is aggrieved successfully establishes such a violation of this chapter or of chapter 119 of this title or of the above specific provisions of title 50, the Court may assess as damages – (1) actual damages, but not less than $10,000, whichever amount is greater; and (2) litigation costs, reasonably incurred.

"(b)(1) Any action against the United States under this section may be commenced only after a claim is presented to the appropriate department or agency under the procedures of the Federal Tort Claims Act, as set forth in title 28, United States Code. (2) Any action against the United States under this section shall be forever barred unless it is presented in writing to the appropriate Federal agency within 2 years after such claim accrues or unless

Consequences: Administrative Action

Upon a judicial or administrative determination that a Title III violation suggesting possible intentional or willful misconduct on the part of a federal officer or employee, the federal agency or department involved may institute disciplinary action. It is required to explain to its Inspector General's office if declines to do so.[61]

Consequences: Attorney Discipline

---

action is begun within 6 months after the date of mailing, by certified or registered mail, of notice of final denial of the claim by the agency to which it was presented. The claim shall accrue on the date upon which the claimant first has a reasonable opportunity to discover the violation. (3) Any action under this section shall be tried to the court without a jury. (4) Notwithstanding any other provision of law, the procedures set forth in section 106(f), 305(g), or 405(f) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) shall be the exclusive means by which materials governed by those sections may be reviewed. (5) An amount equal to any award against the United States under this section shall be reimbursed by the department or agency concerned to the fund described in section 1304 of title 31, United States Code, out of any appropriation, fund, or other account (excluding any part of such appropriation, fund, or account that is available for the enforcement of any Federal law) that is available for the operating expenses of the department or agency concerned.

(c) [Administrative discipline]

"(d) Any action against the United States under this subsection shall be the exclusive remedy against the United States for any claims within the purview of this section.

"(e) (1) Upon the motion of the United States, the court shall stay any action commenced under this section if the court determines that civil discovery will adversely affect the ability of the Government to conduct a related investigation or the prosecution of a related criminal case. Such a stay shall toll the limitations periods of paragraph (2) of subsection (b). (2) In this subsection, the terms 'related criminal case' and 'related investigation' mean an actual prosecution or investigation in progress at the time at which the request for the stay or any subsequent motion to lift the stay is made. In determining whether an investigation or a criminal case is related to an action commenced under this section, the court shall consider the degree of similarity between the parties, witnesses, facts, and circumstances involved in the 2 proceedings, without requiring that any one or more factors be identical. (3) In requesting a stay under paragraph (1), the Government may, in appropriate cases, submit evidence ex parte in order to avoid disclosing any matter that may adversely affect a related investigation or a related criminal case. If the Government makes such an ex parte submission, the plaintiff shall be given an opportunity to make a submission to the court, not ex parte, and the court may, in its discretion, request further information from either party," 18 U.S.C. 2712. Section 2712 expires on December 31, 2005 with the other USA PATRIOT Act provisions that sunset on that date, 115 Stat. 295 (2001).

[61] "If a court or appropriate department or agency determines that the United States or any of its departments or agencies has violated any provision of this chapter, and the court or appropriate department or agency finds that the circumstances surrounding the violation raise serious questions about whether or not an officer or employee of the United States acted willfully or intentionally with respect to the violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly initiate a proceeding to determine whether disciplinary action against the officer or employee is warranted. If the head of the department or agency involved determines that disciplinary action is not warranted, he or she shall notify the Inspector General with jurisdiction over the department or agency concerned and shall provide the Inspector General with the reasons for such determination," 18 U.S.C. 2520(f).

Until recently, the American Bar Association (ABA) considered it ethical misconduct for an attorney to intercept or record a conversation without the consent of all of the parties to the conversation, ABA Formal Op. 337 (1974). The reaction of state regulatory authorities with the power to discipline professional misconduct was mixed. Some agree with the ABA.[62] Some agree with the ABA but have expanded the circumstances under which recording may be conducted within ethical bounds.[63] Some reject the ABA view.[64] The ABA has now repudiated its earlier position, ABA Formal Op. 01-422 (2001). Attorneys who engage in *unlawful* wiretapping or electronic eavesdropping will remain subject to professional discipline in every jurisdiction; in light of the ABA's change of position, it remains to be seen to how state regulatory authorities will react to *lawful* wiretapping or electronic eavesdropping by members of the bar.

---

[62] *Ala. Opinion 84-22* (1984); *People v. Smith*, 778 P.2d 685, 686, 687 (Colo. 1989); *Haw. Formal Opinion No. 30* (1988); *Ind.State Bar Ass'n Op.No.1* (2000); *Iowa State Bar Ass'n v. Mollman*, 488 N.W.2d 168, 169-70, 171-72 (Iowa 1992); *Mo.Advisory Comm. Op. Misc. 30* (1978); *Tex.Stat.Bar Op. 514* (1996); *Va. LEO #1635* (1995), *Va. LEO #1324*; *Gunter v. Virginia State Bar*, 238 Va. 617, 621-22, 385 S.E.2d 597, 600 (1989).

Thus far, the federal courts seem to be in accord, *Parrott v. Wilson*, 707 F.2d 1262 (11th Cir. 1983); *Moody v. IRS*, 654 F.2d 795 (D.C. Cir. 1981); *Ward v. Maritz, Inc.*, 156 F.R.D. 592 (D.N.J. 1994); *Wilson v. Lamb*, 125 F.R.D. 142 (E.D.Ky. 1989); *Haigh V. Matsushita Electric Corp.*, 676 F.Supp. 1332 (E.D.Va. 1987).

[63] *Ariz. Opinion No. 95-03* (1995); *Alaska Bar Ass'n Eth.Comm. Ethics Opinions No. 95-5 (1995) and No. 91-4* (1991); *Idaho Formal Opinion 130* (1989); *Kan.Bar.Ass'n Opinion 96-9* (1997); *Ky.Opinion E-279* (1984); *Minn.Law.Prof. Resp.Bd. Opinion No. 18* (1996); *Ohio Bd.Com.Griev.Disp. Opinion No. 97-3* (1997); *S.C. Ethics Advisory Opinion 92-17* (1992); *Tenn.Bd.Prof.Resp. Formal Ethics Opinion No. 86-F-14(a)* (1986).

[64] *D.C. Opinion No. 229* (1992) (recording was not unethical because it occurred under circumstances in which the uninformed party should have anticipated that the conversation would be recorded or otherwise memorialized); *Mississippi Bar v. Attorney ST.*, 621 So.2d 229 (Miss. 1993)(context of the circumstances test); *Conn.Bar Ass''n Op. 98-9* (1998)(same); *Mich.State Bar Op. RI-309* (1998)(same); *Me.State Bar Op.No. 168* (1999)(same); *N.M.Opinion 1996-2* (1996)(members of the bar are advised that there are no clear guidelines and that the prudent attorney avoids surreptitious recording); *N.C. RPC 171* (1994)(lawyers are encouraged to disclose to the other lawyer that a conversation is being tape recorded); *Okla.Bar Ass'n Opinion* 307 (1994)(a lawyer may secretly recording his or her conversations without the knowledge or consent of other parties to the conversation unless the recording is unlawful or in violation of some ethical standard involving more than simply recording); *Ore.State Bar Ass'n Formal Opinion No. 1991-74* (1991) (an attorney with one party consent he or she may record a telephone conversation "in absence of conduct which would reasonably lead an individual to believe that no recording would be made"); *Utah State Bar Ethics Advisory Opinion No. 96-04* (1996) ("recording conversations to which an attorney is a party without prior disclosure to the other parties is not unethical when the act, considered within the context of the circumstances, does not involve dishonesty, fraud, deceit or misrepresentation"); *Wis.Opinion E-94-5* ("whether the secret recording of a telephone conversation by a lawyer involves 'dishonesty, fraud, deceit or misrepresentation' under SCR 20:8.4(c) depends upon all the circumstances operating at the time"). In New York, the question of whether an attorney's surreptitiously recording conversations is ethically suspect is determined by locality, compare, *Ass'n of the Bar of City of N.Y. Formal Opinion No. 1995-10* (1995)(secret recording is per se unethical), with, *N.Y.County Lawyer's Ass'n Opinion No. 696* (1993)(secret recording is not per se unethical).

Consequences: Exclusion of evidence

Information whose disclosure is prohibited by the federal wiretapping statute is inadmissible as evidence before any federal, state, or local tribunal or authority, 18 U.S.C. 2515.[65] The benefits of the section 2515 exclusionary rule may be claimed through a motion to suppress under 18 U.S.C. 2518(10)(a).[66]

Although the Supreme Court has held that section 2515 may require suppression in instances where the Fourth Amendment exclusionary rule would not, *Gelbard v. United States*, 408 U.S. 41, 52 (1972), some of the lower courts have recognized the applicability of the good faith exception to the Fourth Amendment exclusionary rule in section 2515 cases.[67] Other courts have held, moreover, that the fruits of an

---

[65] "Whenever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof if the disclosure of that information would be in violation of this chapter," 18 U.S.C. 2515.

[66] "Any aggrieved person in any trial, hearing, or proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the contents of any wire or oral communication intercepted pursuant to this chapter, or evidence derived therefrom, on the grounds that – (i) the communication was unlawfully intercepted; (ii) the order of authorization or approval under which it was intercepted is insufficient on its face; or (iii) the interception was not made in conformity with the order of authorization or approval.

"Such motion shall be made before the trial, hearing, or proceeding unless there was no opportunity to make such motion or the person was not aware of the grounds of the motion. If the motion is granted, the contents of the intercepted wire or oral communication, or evidence derived therefrom, shall be treated as having been obtained in violation of this chapter. The judge, upon the filing of such motion by the aggrieved person, may in his discretion make available to the aggrieved person or his counsel for inspection such portions of the intercepted communication or evidence derived therefrom as the judge determines to be in the interests of justice," 18 U.S.C. 2518(10)(a).

"The Supreme Court has explained the relationship between these two provisions. In *United States v. Giordano*, 416 U.S. 505 (1974), the Court wrote that 'what disclosures are forbidden under 2515 and we subject to motions to suppress is . . . governed by 2518(10(a).' Thus, evidence may be suppressed only if one of the grounds set out in 2518(10)(a) is met. Moreover not every failure to comply fully with any requirement provided in Title III would render the interception of wire or oral communications unlawful under 2518(10)(a)(i). *United States v. Donovan*, 429 U.S. 413, 433 (1977), quoting *United States v. Chavez*, 416 U.S. 562 (1974). Rather suppression is mandated only for a failure to satisfy any of those statutory requirements that directly and substantially implement the congressional intention to limit the use of intercept procedures to those situations clearly calling for the employment of this extraordinary investigative device, *Donovan*, 429 U.S. at 433-34, quoting *Girodano*, 416 U.S. at 527," *United States v. Williams*, 124 F.3d 411, 426 (3d Cir. 1997); *United States v. Escobar-deJesus*, 187 F.3d 148, 171 (1st Cir. 1999).

[67] *United States v. Moore*, 41 F.3d 370, 376 (8th Cir. 1994); *United States v. Ambrosio*, 898 F.Supp. 177, 187 (S.D.N.Y. 1995); *United States v. Malelzadeh*, 855 F.2d 1492, 1497 (11th Cir. 1988).

Gelbard held that a grand jury witness might claim the protection of section 2515 through a refusal to answer questions based upon an unlawful wiretap notwithstanding the

unlawful wiretapping or electronic eavesdropping may be used for impeachment purposes.[68]

The admissibility of tapes or transcripts of tapes of intercepted conversations raise a number of questions quite apart from the legality of the interception. As a consequence of the prerequisites required for admission, privately recorded conversations are more likely to be found inadmissible than those recorded by government officials. Admissibility will require the party moving admission to show that the tapes or transcripts are accurate, authentic and trustworthy.[69] For some courts this demands a showing that, "(1) the recording device was capable of recording the events offered in evidence; (2) the operator was competent to operate the device; (3) the recording is authentic and correct; (4) changes, additions, or deletions have not been made in the recording; (5) the recording has been preserved in a manner that is shown to the court; (6) the speakers on the tape are identified; and (7) the conversation elicited was made voluntarily and in good faith, without any kind of inducement."[70]

Illegal Disclosure of Information Obtained by Wiretapping or Electronic Eavesdropping

Although often overlooked, it also a federal crime to disclose information obtained from illicit wiretapping or electronic eavesdropping, 18 U.S.C. 2511(1)(c):

---

fact that the Fourth Amendment exclusionary rule does not apply in grand jury proceedings. The good faith exception to the Fourth Amendment exclusionary rule permits the admission of evidence secured in violation of the Fourth Amendment, if the officers responsible for the breach were acting in good faith reliance upon the apparent authority of a search warrant or some like condition negating the remedial force of the rule, *United States v. Leon*, 468 U.S. 431, 446-48 (1984).

[68] *Culbertson v. Culbertson*, 143 F.3d 825, 827-28 (4th Cir. 1998); *United States v. Echavarria-Olarte*, 904 F.2d 1391 (9th Cir. 1990); *United States v. Vest*, 813 F.2d 477, 484 (1st Cir. 1987).

[69] *United States v. Thompson,* 130 F.3d 676, 683 (5th Cir. 1997); *United States v. Panaro*, 241 F.3d 1104, 1111 (9th Cir. 2001); *United States v. Smith*, 242 F.3d 737, 741 (7th Cir. 2001);.

[70] *United States v. Webster*, 84 F.3d 1056, 1064 (8th Cir. 1996); *United States v. Green*, 175 F.3d 822, 830 n.3 (10th Cir. 1999); *cf., United States v. Calderin-Rodriguez*, 244 F.3d 977, 986-87 (8th Cir. 2001). These seven factors have been fairly widely cited since they were first announced in *United States v. McKeever*, 169 F.Supp 426, 430 (S.D.N.Y. 1958), *rev'd on other grounds*, 271 F.2d 669 (2d Cir. 1959). They are a bit formalistic for some courts who endorse a more ad hoc approach to the assessment of whether the admission of what purports to be a taped conversation will introduce fraud or confusion into the court, *see e.g.*, *Stringel v. Methodist Hosp. of Indiana, Inc.*, 89 F.3d 415, 420 (7th Cir. 1996)(*McKeever* "sets out a rather formal, seven step checklist for the authentication of tape recordings, and we have looked to some of the features [in the past]"); *United States v. White*, 116 F.3d 903, 921 (D.C.Cir. 1997)("tapes may be authenticated by testimony describing the process or system that created the tape or by testimony from parties to the conversation affirming that the tapes contained an accurate record of what was said"); *United States v. Tropeano*, 252 F.3d 653, 661 (2d Cir. 2001)("[T]his Circuit has never expressly adopted a rigid standard for determining the admissibility of tape recordings"); *United States v. Westmoreland*, 312 F.3d 302, 310-11 (7th Cir. 2002).

- any person [who]
- intentionally
- discloses or endeavors to disclose to another person
- the contents of any wire, oral, or electronic communication
- having reason to know
- that the information was obtained through the interception of a wire, oral, or electronic communication
- in violation of 18 U.S.C. 2511(1)
- is subject to the same sanctions and remedies as the wiretapper or electronic eavesdropper.

This is true of the wiretapper or electronic eavesdropper and of all those who disclose information, that in fact can be traced to a disclosure by the original wiretapper or eavesdropper, with reason to know of the information's illicit origins, except to the extent the First Amendment bans application.[71] The legislative history speaks of a common knowledge limitation on the statute's coverage, but it is not clear whether it refers to common knowledge at the time of interception or at the time disclosure, S.REP.NO. 1097, 90th Cong., 2d Sess. 93 (1967).[72] By definition a violation of paragraph 2511(1)(c) requires an earlier unlawful interception under subsection 2511(1). If there is no predicate unlawful interception there can be no violation of paragraph 2511(1)(c).

The results of electronic eavesdropping authorized under Title III/ECPA may be disclosed and used for law enforcement purposes [73] and for testimonial purposes.[74]

---

[71] *Bartnicki v. Vopper*, 532 U.S. 514, 533-34 (2001), pointed out that the First Amendment right to free speech bars the application of section 2511(1)(c) to the disclosure of illegally intercepted, but lawfully acquired, communications dealing with a matter of unusual public concern. Bartnicki was a union negotiator whose telephone conversations with the union's president were surreptitiously intercepted and recorded while they were discussion negotiation of a teachers' contract. During the conversation, the possibility of using violence against school board members was mentioned. After the teachers' contract was signed, the unknown wiretapper secretly supplied Yocum, a critic of the union's position, with a copy of the tape. Yocum in turn played it for members of the school board and turned it over to Vopper, a radio talk show host, who played it on his show. Other stations and media outlets published the contents as well. Bartnicki sued Vopper and Yocum for use and disclosure in violation of sections 2511(1)(c) and 2511(1)(d). Vopper and Yocum offered a free speech defense which the Supreme Court accepted. For a more extensive examination of *Bartnicki, see*, Featherstone, *The Right to Publish Lawfully Obtained But Illegally Intercepted Material of Public Concern: Bartnicki v. Vopper*, CRS Report RS20974 (July, 2001).

[72] "Subparagraphs (c) and (d) prohibit, in turn, the disclosure or use of the contents of any intercepted communication by any person knowing or having reason to know the information was obtained through an interception in violation of this subsection. The disclosure of the contents of an intercepted communication that had already become 'public information' or 'common knowledge' would not be prohibited. The scope of this knowledge required to violate either subparagraph reflects existing law (*Pereira v. United States*, 347 U.S. 1 (1954)." The remark may also have been influenced by the high level of intent (willfully rather than intentionally) included in the disclosure provision as reported out.

[73] "Any investigative or law enforcement officer who, by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic

It is also a federal crime to disclose, with an intent to obstruct criminal justice, any information derived from lawful police wiretapping or electronic eavesdropping, *i.e.*:

• any person [who]
• intentionally discloses, or endeavors to disclose, to any other person
•the contents of any wire, oral, or electronic communication
• intercepted by means authorized by sections:
- 2511(2)(a)(ii) (communication service providers, landlords, etc. who assist police setting up wiretaps or electronic eavesdropping devices
- 2511(2)(b) (FCC regulatory activity)
- 2511(2)(c) (police one party consent)
- 2511(2)(e) (Foreign Intelligence Surveillance Act)
- 2516 (court ordered, police wiretapping or electronic surveillance)
- 2518 (emergency wiretaps or electronic surveillance)
• knowing or having reason to know that
• the information was obtained through the interception of such a communication
• in connection with a criminal investigation
• having obtained or received the information in connection with a criminal investigation
• with intent to improperly obstruct, impede, or interfere with a duly authorized criminal investigation,
•is subject to the same sanctions and remedies as one who illegally wiretaps, 18 U.S.C. 2511(1)(e).[75]

---

communication, or evidence derived therefrom, may disclose such contents to another investigative or law enforcement officer to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure," 18 U.S.C. 2517(1).

[74] "Any person who has received, by any means authorized by this chapter, any information concerning a wire, oral, or electronic communication, or evidence derived therefrom intercepted in accordance with the provisions of this chapter may disclose the contents of that communication or such derivative evidence while giving testimony under oath or affirmation in any proceeding held under the authority of the United States or of any State or political subdivision thereof," 18 U.S.C. 2517(3). This does not entitle private litigants to disclosure in the view of at least one court, *In re Motion to Unseal Electronic Surveillance Evidence*, 990 F.2d 1015 (8th Cir. 1993).

When court ordered interception results in evidence of a crime other than the crime with respect to which the order was issued, the evidence is admissible only upon a judicial finding that it was otherwise secured in compliance with Title III/ECPA requirements, 18 U.S.C. 2517(5).

[75] When acting with a similar intent, disclosure of the *fact* of authorized federal wiretap or foreign intelligence gathering is proscribed elsewhere in title 18. "Whoever, having knowledge that a Federal investigative or law enforcement officer has been authorized or has applied for authorization under chapter 119 to intercept a wire, oral, or electronic communication, in order to obstruct, impede, or prevent such interception, gives notice or attempts to give notice of the possible interception to any person shall be fined under this title or imprisoned not more than five years, or both."

"Whoever, having knowledge that a Federal officer has been authorized or has applied for authorization to conduct electronic surveillance under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801, et seq.), in order to obstruct, impede, or prevent such activity, gives notice or attempts to give notice of the possible activity to any person

The proscriptions 2511(1)(e) would appear to apply to efforts to obstruct justice by information gleaned from either federal or state police wiretaps. Use of the word "authorized" in conjunction with a list of federal statutes might suggest that the paragraph was only intended to protect wiretap information gathered by federal rather than by federal or state authorities. But most of the cited sections do not "authorize" anything; they simply confine the reach of the statutory prohibitions. And several are as likely to involve state interceptions as federal, e.g., the one-party-consent-under-color-of-law interceptions.

Essentially, the same consequence flow from an unlawful disclosure under paragraphs 2511(1)(c) or 2511(1)(e) as follow unlawful interception under paragraphs 2511(1)(a) or 2511(1)(b):

- maximum 5 year prison terms and fines of not more than $250,000 or $500,000 depending upon whether the offender is an individual or organization;[76]

- exposure to civil liability including equitable relief and actual or statutory damages.[77]

Illegal Use of Information Obtained by Unlawful Wiretapping or Electronic Eavesdropping

The prohibition on the use of information secured from illegal wiretapping or electronic eavesdropping mirrors the disclosure provision, 18 U.S.C. 2511(1)(d):

- any person [who]
- intentionally
- uses or endeavors to use to another person
- the contents of any wire, oral, or electronic communication
- having reason to know
- that the information was obtained through the interception of a wire, oral, or electronic communication
- in violation of 18 U.S.C. 2511(1)

---

shall be fined under this title or imprisoned not more than five years, or both," 18 U.S.C. 2232(d),(e).

[76] "[W]hoever violates subsection (1) of this section shall be fined under this title or imprisoned not more than five years, or both," 18 U.S.C. 2511(4)(a).

[77] "(a) . . . any person whose wire, oral, or electronic communication is . . . disclosed . . . used in violation of this chapter may in a civil action recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate. . . .(g) Any willful disclosure . . . by an investigative or law enforcement officer or governmental entity of information beyond the extent permitted by section 2517 is a violation of this chapter for purposes of section 2520(a)," 18 U.S.C. 2520(a),(g).

• is subject to the same sanctions and remedies as the wiretapper or electronic eavesdropper.

The available case law under the use prohibition of section 2511(1)(d) is scant, and the section has rarely been invoked except in conjunction with the disclosure prohibition of section 2511(c). The wording of the two is clearly parallel, the legislative history describes them in the same breath,[78] and they are treated alike for law enforcement purposes.[79] *Bartnicki* seems destined to change all that, because it appears to parse the constitutionally suspect ban on disclosure from constitutionally permissible ban on use.[80] In doing so, it may also resolve a conflict among the lower federal appellate courts over the so-called "clean hands" exception. A few courts had recognized an exception to the disclosure-use bans of section 2511(1) where law enforcement officials might disclose or use the results of an illegal interception in which they had played no role.[81] *Bartnicki* appears to dim the prospects of a clean hands exception when, to illustrate situations to which the section 2511(1)(d) use ban might be applied constitutionally, it points to one of the cases which rejected to the exception.[82]

The consequences of unlawful use of intercepted communications in violation of paragraph 2511(d) are similar to those for unlawful disclosure in violation of paragraphs 2511(1)(c) or 2511(1)(e), or for follow unlawful interception under paragraphs 2511(1)(a) or 2511(1)(b):

---

[78] "Subparagraphs (c) and (d) prohibit, in turn, the disclosure or use of the contents of any intercepted communication by any person knowing or having reason to know the information was obtained through an interception in violation of this subsection," S.REP.NO. 1097, 90th Cong., 2d Sess. 93 (1967).

[79] *Compare*, 18 U.S.C. 2517(1)("Any investigative or law enforcement officer who, by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents to another investigative or law enforcement officer to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure"), *with* 18 U.S.C. 2517(2)("Any investigative or law enforcement officer who, by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication or evidence derived therefrom may use such contents to the extent such use is appropriate to the proper performance of his official duties").

[80] "[T]he naked prohibition against disclosures is fairly characterized as a regulation of pure speech. Unlike the prohibition against the 'use' of the contents of an illegal interception in §2511(1)(d), subsection (c) is not a regulation of conduct," 532 U.S. at 526-27.

[81] *Forsyth v. Barr*, 19 F.3d 1527, 1541-545 (5th Cir. 1994); *United States v. Murdock*, 63 F.3d 1391, 1400-403 (6th Cir. 1995); *contra*, *Berry v. Funk*, 146 F.3d 1003, 1011-13 (D.C.Cir. 1998); *Chandler v. United States Army*, 125 F.3d 1296, 1300-302 (9th Cir. 1997); *In re Grand Jury*, 111 F.3d 1066, 1077 (3d Cir. 1997); *United States v. Vest*, 813 F.2d 477, 481 (1st Cir. 1987).

[82] "Unlike the prohibition against the 'use' of the contents of an illegal interception in §2511(1)(d),* subsection (c) is not a regulation of conduct.

*"The Solicitor General has catalogued some of the cases that fall under subsection(d): . . . . The statute has also been held to bar the use of illegally intercepted communications for important and socially valuable purposes, see, *In re Grand Jury* , 111 F.3d 1066, 1077-79 (3d Cir. 1997)," 532 U.S. at 527(footnote 10 of the Court's opinion quoted after the *).

- maximum 5 year prison terms and fines of not more than $250,000 or $500,000 depending upon whether the offender is an individual or organization;[83]

- exposure to civil liability including equitable relief and actual or statutory damages.[84]

Shipping, Manufacturing, Distributing, Possessing or Advertising Wire, Oral, or Electronic Communication Interception Devices

The proscriptions for possession and trafficking in wiretapping and eavesdropping devices are even more demanding than those that apply to the predicate offense itself. There are exemptions for service providers,[85] government officials and those under contract with the government,[86] but there is no exemption for equipment designed to be used by private individuals, lawfully but surreptitiously.[87]

---

[83] "[W]hoever violates subsection (1) of this section shall be fined under this title or imprisoned not more than five years, or both," 18 U.S.C. 2511(4)(a).

[84] "(a) . . . any person whose wire, oral, or electronic communication is . . . intentionally used in violation of this chapter may in a civil action recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate. . . .(g) Any willful . . . use by an investigative or law enforcement officer or governmental entity of information beyond the extent permitted by section 2517 is a violation of this chapter for purposes of section 2520(a)," 18 U.S.C. 2520(a),(g).

[85] "It shall not be unlawful under this section for – (a) a provider of wire or electronic communication service or an officer, agent, or employee of, or a person under contract with, such a provider, in the normal course of the business of providing that wire or electronic communication service . . . to send through the mail, send or carry in interstate or foreign commerce, or manufacture, assemble, possess, or sell any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications," 18 U.S.C. 2512(2)(a).

[86] "(2) It shall not be unlawful under this section for . . . (b) an officer, agent, or employee of, or a person under contract with, the United States, a State, or a political subdivision thereof, in the normal course of the activities of the United States, a State, or a political subdivision thereof, to send through the mail, send or carry in interstate or foreign commerce, or manufacture, assemble, possess, or sell any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications.

"(3) It shall not be unlawful under this section to advertise for sale a device described in subsection (1) of this section if the advertisement is mailed, sent, or carried in interstate or foreign commerce solely to a domestic provider of wire or electronic communication service or to an agency of the United States, a State, or a political subdivision thereof which is duly authorized to use such device," 18 U.S.C. 2512(2)(b),(3).

[87] *United States v. Spy Factory, Inc.*, 961 F.Supp. 450, 473-75 (S.D.N.Y. 1997); *United States v. Bast*, 495 F.2d 138, 141 (D.C.Cir. 1974).

The three prohibitions in section 2512 present generally common features, declaring that:

• any person who

• intentionally

• either

(a)

- sends through the mail or sends or carries in interstate or foreign commerce
- any electronic, mechanical, or other device
- knowing or having reason to know
- that the design of such device renders it primarily useful
- for the purpose of the surreptitious interception of wire, oral, or electronic communications; or

(b)

- manufactures, assembles, possesses, or sells
- any electronic, mechanical, or other device
- knowing or having reason to know
- that the design of such device renders it primarily useful
- for the purpose of the surreptitious interception of wire, oral, or electronic communications, and
- that such device or any component thereof has been or will be sent through the mail or transported in interstate or foreign commerce; or

(c)

- places in any newspaper, magazine, handbill, or other publication *or disseminates electronically*
- any advertisement of –
    + any electronic, mechanical, or other device
    + knowing or having reason to know
    + that the design of such device renders it primarily useful
    + for the purpose of the surreptitious interception of wire, oral, or electronic communications; or
    + any other electronic, mechanical, or other device
    + where such advertisement promotes the use of such device
    + for the purpose of the surreptitious interception of wire, oral, or electronic communications
- *knowing the content of the advertisement and* knowing or having reason to know
- that such advertisement will be sent through the mail or transported in interstate or foreign commerce

• shall imprisoned for not more than 5 years and/or fined not more than $250,000 (not more than $500,000 for organizations), 18 U.S.C. 2512.[88]

The legislative history lists among the items Congress considered "primarily useful for the purpose of the surreptitious interception of communications: the martini olive transmitter, the spike mike, the infinity transmitter, and the microphone disguised as a wristwatch, picture frame, cuff link, tie clip, fountain pen, stapler, or cigarette pack," S.REP.NO. 1097, 90th Cong., 2d Sess. 95 (1968).

Questions once raised over whether section 2512 covers equipment designed to permit unauthorized reception of scrambled satellite television signals have been resolved.[89] Each of the circuits to consider the question have now concluded that 2512 outlaws such devices.[90] Their use is also proscribed by 47 U.S.C. 605.[91]

---

[88] The Homeland Security Act amended (italics) section 2512 to cover advertisements using the Internet and other electronic means, 116 Stat. 2158 (2002).

[89] The two appellate panel decisions that found the devices beyond the bounds of section 2512, *United States v. Herring*, 933 F.2d 932 (11th Cir. 1991) and *United States v. Hux*, 940 F.2d 314 (8th Cir. 1991) have been overturned en banc, *United States v. Herring*, 993 F.2d 784, 786 (11th Cir. 1993); *United States v. Davis*, 978 F.2d 415, 416 (8th Cir. 1992).

[90] *United States v. Harrell*, 983 F.2d 36, 37-9 (5th Cir. 1993); *United States v. One Macom Video Cipher II*, 985 F.2d 258, 259-61 (6th Cir. 1993); *United States v. Shriver*, 989 F.2d. 898, 901-906 (7th Cir. 1992); *United States v. Davis*, 978 F.2d 415, 417-20 (8th Cir. 1992); *United States v. Lande*, 968 F.2d 907, 910-11 (9th Cir. 1992); *United States v. McNutt*, 908 F.2d 561, 564-65 (10th Cir. 1990); *United States v. Herring*, 993 F.2d 784, 786-89 (11th Cir. 1991).

[91] "(a). . . No person not being entitled thereto shall receive or assist in receiving any interstate or foreign communication by radio and use such communication (or any information therein contained) for his own benefit or for the benefit of another not entitled thereto. No person having received any intercepted radio communication or having become acquainted with the contents, substance, purport, effect, or meaning of such communication (or any part thereof) knowing that such communication was intercepted, shall divulge or publish the existence, contents, substance, purport, effect, or meaning of such communication (or any part thereof) or use such communication (or any information therein contained) for his own benefit or for the benefit of another not entitled thereto. This section shall not apply to the receiving, divulging, publishing, or utilizing the contents of any radio communication which is transmitted by any station for the use of the general public, which relates to ships, aircraft, vehicles, or persons in distress, or which is transmitted by an amateur radio station operator or by a citizens band radio operator.

"(b) The provisions of subsection (a) of this section shall not apply to the interception or receipt by any individual, or the assisting (including the manufacture or sale) of such interception or receipt, of any satellite cable programming for private viewing if – (1) the programming involved is not encrypted; and (2)(A) a marketing system is not established under which – (i) an agent or agents have been lawfully designated for the purpose of authorizing private viewing by individuals, and
(ii) such authorization is available to the individual involved from the appropriate agent or agents; or (B) a marketing system described in subparagraph (A) is established and the individuals receiving such programming has obtained authorization for private viewing under that system . . .

"(2) Any person who violates subsection (a) of this section willfully and for purposes of direct or indirect commercial advantage or private financial gain shall be fined not more than $50,000 or imprisoned for not more than 2 years, or both, for the first such conviction

Stored Electronic Communications

In its original form Title III was ill suited to ensure the privacy of those varieties of modern communications which are equally vulnerable to intrusion when they are at rest as when they are in transmission. Surreptitious "access" is as least as great a threat as surreptitious "interception" to the patrons of electronic mail (e-mail), electronic bulletin boards, voice mail, pagers, and remote computer storage.

Accordingly, Title III/ECPA also bans surreptitious access to communications at rest, although it does so beyond the confines of that apply to interception, 18 U.S.C. 2701 - 2711.[92] These separate provisions afford protection for e-mail, voice

---

and shall be fined not more than $100,000 or imprisoned for not more than 5 years, or both, for any subsequent conviction.

"(3)(A) Any person aggrieved by any violation of subsection (a) of this section or paragraph (4) of this subsection may bring a civil action in a United States district court or in any other court of competent jurisdiction. (B) The court – (i) may grant temporary and final injunctions on such terms as it may deem reasonable to prevent or restrain violations of subsection (a) of this section; (ii) may award damages as described in subparagraph (C); and (iii) shall direct the recovery of full costs, including awarding reasonable attorneys' fees to an aggrieved party who prevails. (C)(i) Damages awarded by any court under this section shall be computed, at the election of the aggrieved party, in accordance with either of the following subclauses: (I) the party aggrieved may recover the actual damages suffered by him as a result of the violation and any profits of the violator that are attributable to the violation which are not taken into account in computing the actual damages; in determining the violator's profits, the party aggrieved shall be required to prove only the violator's gross revenue, and the violator shall be required to prove his deductible expenses and the elements of profit attributable to factors other than the violation; or (II) the party aggrieved may recover an award of statutory damages for each violation of subsection (a) of this section involved in the action in a sum of not less than $1,000 or more than $10,000, as the court considers just, and for each violation of paragraph (4) of this subsection involved in the action an aggrieved party may recover statutory damages in a sum not less than $10,000, or more than $100,000, as the court considers just. (ii) In any case in which the court finds that the violation was committed willfully and for purposes of direct or indirect commercial advantage or private financial gain, the court in its discretion may increase the award of damages, whether actual or statutory, by an amount of not more than $100,000 for each violation of subsection (a) of this section. (iii) In any case where the court finds that the violator was not aware and had no reason to believe that his acts constituted a violation of this section, the court in its discretion may reduce the award of damages to a sum of not less than $250.

"(4) Any person who manufactures, assembles, modifies, imports, exports, sells, or distributes any electronic, mechanical, or other device or equipment, knowing or having reason to know that the device or equipment is primarily of assistance in the unauthorized decryption of satellite cable programming, or direct-to-home satellite services, or is intended for any other activity prohibited by subsection (a) of this section, shall be fined not more than $500,000 for each violation, or imprisoned for not more than 5 years for each violation, or both. For purposes of all penalties and remedies established for violations of this paragraph, the prohibited activity established herein as it applies to each such device shall be deemed a separate violation. . . ."

[92] The courts differ somewhat over the circumstances under which stored communications can be "intercepted" and thus subject to the protection of Title III as well, *compare, United States v. Smith*, 155 F.3d 1051, 1058 (9th Cir. 1998)(unauthorized retrieval and recording of another's voice mail messages constitutes an "interception"); *Konop v. Hawaiian Airlines,*

mail, and other electronic communications somewhat akin to that available for telephone and face to face conversations under 18 U.S.C. 2510-2522. Thus, subject to certain exceptions, it is a federal crime to:

- intentionally
- either
  - access without authorization or
  - exceed an authorization to access
- a facility through which an electronic communication service is provided
- and thereby obtain, alter, or prevent authorized access to a wire or electronic communication while it is in electronic storage in such system, 18 U.S.C. 2701(a).

The exceptions cover electronic storage facility operators, their customers, and –under procedural counterparts to court ordered wiretapping – governmental entities.[93]

Violations committed for malicious, mercenary, tortious or criminal purposes are punishable by imprisonment for not more than 5 years and/or a fine of not more than $250,000 (not more than 10 years for a subsequent conviction); lesser transgressions, by imprisonment for not more than 1 year (not more than 5 years for

---

Inc., 236 F.3d 1035, 1046 (9th Cir. 2001)(fraudulent access to a secure website constitutes an "interception;" electronic communications are entitled to the same protection when they are in storage as when are in transit); *Fraser v. National Mutual Insurance Co.*, 135 F.Supp.2d 623, 634-37 (E.D.Pa. 2001)(""interception" of e-mail occurs with its unauthorized acquisition prior to initial receipt by its addressee); *with, Steve Jackson Games, Inc. v. United States Secret Service*, 36 F.3d 457, 461-62n.7 (5th Cir. 1994) (Congress did not intend for "interception" to apply to e-mail stored on an electronic bulletin board; stored wire communications (voice mail), however, is protected from "interception"); *United States v. Meriwether*, 917 F.2d 955, 959-60 (6th Cir. 1990)(access to stored information through the use another's pager does not constitute an "interception"); *United States v. Reyes,* 922 F.Supp. 818, 836-37 (S.D.N.Y. 1996)(same); *Wesley College v. Pitts*, 947 F.Supp. 375, 385 (D.Del. 1997)(no "interception" occurs when the contents of electronic communications are acquired unless contemporaneous with their transmission); *see also, Adams v. Battle Creek*, 250 F.3d 980, 982 (6th Cir. 2001)(use of a "clone" or duplicate pager to simultaneously receive the same message as a target pager is an "interception"); *Brown v. Waddell*, 50 F.3d 285, 294 (4th Cir. 1995)(same). The USA PATRIOT Act resolved some of the uncertainty when it removed voice mail from the coverage of Title III, 115 Stat. 283 (2001)(striking the phrase "and such term includes any electronic storage of such communication" from the definition of "wire communications" in Title III (18 U.S.C. 2510(1)) and adding stored wire communications to the stored communications coverage of 18 U.S.C. 2703 – changes that will disappear with the other USA PATRIOT Act amendments that sunset on December 31, 2005, 115 Stat. 295 (2001)).

[93] "Subsection (a) of this section does not apply with respect to conduct authorized – (1) by the person or entity providing a wire or electronic communications service; (2) by a user of that service with respect to a communication of or intended for that user; or (3) in section 2703 [requirements for government access], 2704 [backup preservation] or 2518 [court ordered wiretapping or electronic eavesdropping] of this title," 18 U.S.C. 2701(c).

Section 2709 creates an exception for counterintelligence access to telephone records.

a subsequent conviction) and/or a fine of not more than $100,000.[94] Those who provide the storage service and other victims of unlawful access have a cause of action for equitable relief, reasonable attorneys' fees and costs, damages equal the loss and gain associated with the offense but not less than $1000.[95] Both criminal and civil liability are subject to good faith defenses.[96]

---

[94] "The punishment for an offense under subsection (a) of this section is – (1) if the offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain, or in furtherance of any criminal or tortious act in violation of the constitution and laws of the United States or any state – (A) a fine under this title or imprisonment for not more than 5 years, or both, in the case of a first offense under this subparagraph; and (B) a fine under this title or imprisonment for not more than 10 years, or both, for any subsequent offense under this subparagraph; and (2)(A) a fine under this title or imprisonment for not more than 1 year or both, in the case of a first offense under this paragraph; and (B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under this subparagraph that occurs after a conviction of another offense under this section."18 U.S.C. 2701(b). The Homeland Security Act rewrote this subsection, 116 Stat. 2158-159 (2002), to increase the penalties, H.Rep.No. 107-497, at 17-8 (2002).

[95] "(a) Cause of action – Except as provided in section 2703(e)[relating to immunity for compliance with judicial process], any provider of electronic communication service, subscriber, or customer aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or entity *other than the United States* which engaged in that violation such relief as may be appropriate.

"(b) Relief – In a civil action under this section, appropriate relief includes – (1) such preliminary and other equitable or declaratory relief as may be appropriate; (2) damages under subsection(c); and (3) a reasonable attorney's fee and other litigation costs reasonably incurred;

"(c) Damages – The court may assess as damages in a civil action under this section the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation, but in no case shall a person entitled to recover receive less than the sum of $1,000. . . ." 18 U.S.C. 2707. The USA PATRIOT Act added the language in italics when it established a separate cause of action for victims of U.S. violations which may also result in administrative disciplinary action against offending U.S. officers or employees, 18 U.S.C. 2712, 2707(d); the additions expire on December 31, 2001 along with the other USA PATRIOT Act amendments that sunset on that date, 115 Stat. 295 (2001).

[96] "A good faith reliance on – (1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization *(including a request of a governmental entity under section 2703(f) of this title)* [relating to an official request to for a service provider preserve evidence]; (2) a request of an investigative or law enforcement officer under section 2518(7) of this title [relating to emergency wiretapping and electronic eavesdropping]; or (3) a good faith determination that section 2511(3) of this title [relating to the circumstances under which an electronic communications provider may divulge the contents of communication] permitted the conduct complained of – is a complete defense to any civil or criminal action brought under this chapter or any other law," 18 U.S.C. 2707(e). The USA PATRIOT Act amend this subsection as noted above to further clarify the extent of the service provider good faith defense.

Service providers, nevertheless, may incur civil liability for unlawful disclosures,[97] unless they can take advantage of any of a fairly extensive list of exceptions and defenses.[98]

Violations by the United States may give rise to a cause of action and may result in disciplinary action against offending officials or employees under the same provisions that apply to U.S. violations of Title III.[99]

Unlawful access to electronic communications may involve violations of several other federal and state laws, including for instance the federal computer fraud and abuse statute, 18 U.S.C. 1030, and state computer abuse statutes.[100]

Pen Registers and Trap and Trace Devices

---

[97] "Except as in subsection (b) – (1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; (2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service – (A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service; and (B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing; *and (3) a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2)) to any government entity*," 18 U.S.C. 2702(a). The USA PATRIOT Act added paragraph (3) to the subsection 2702(a), 115 Stat. 284 (2001), an amendment that expires on December 31, 2001, 115 Stat. 295 (2001).

Section 2702 makes no mention of any consequences that follow a breach of its commands, but 2707 establishes a civil cause of action for the victims of any violation of chapter 121 (18 U.S.C. 2701 - 2711).

[98] "A person or entity may divulge the contents of a communication – (1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient; (2) as otherwise authorized in section 2517, 2511(2)(a), or 2703 of this title; (3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service; (4) to a person employed or authorized or whose facilities are used to forward such communication to its destination; (5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service; or (6) to a law enforcement agency, if such contents – (A) were inadvertently obtained by the service provider; and (B) appear to pertain to the commission of a crime," 18 U.S.C. 2702(b).

[99] "Any person who is aggrieved by any willful violation this chapter or of chapter 119 of this title [18 U.S.C. 2510-2520] . . . may commence an action in United States District Court . . . .If . . . any of the departments or agencies has violated any provision of this chapter . . . the department or agency shall . . . promptly initiate a proceeding to determine whether disciplinary action . . . is warranted. . . ."18 U.S.C. 2712(a),(c).

[100] Citations to the various state computer abuse statutes are appended.

A trap and trace device identifies the source of incoming calls, and a pen register indicates the numbers called from a particular phone.[101] Since neither allows the eavesdropper to overhear the "contents" of the phone conversation they were not interceptions within the reach of Title III prior to the enactment of ECPA, *United States v. New York Telephone Co.*, 434 U.S. 160 (1977). Although Congress elected to expand the definition of interception, it chose to continue to regulate these devices beyond the boundaries of Title III, 18 U.S.C. 3121 - 3127. The USA PATRIOT Act enlarged the coverage of sections 3121-3127 to include sender/addressee information relating to e-mail and other forms of electronic communications, 115 Stat. 288-91 (2001). Unlike many of the other USA PATRIOT Act's amendments, this one does *not* sunset on December 31, 2005, 115 Stat. 295 (2001).

The use or installation of pen registers or trap and trace devices by anyone other than the telephone company, service provider, or those acting under judicial authority, however, is a federal crime, punishable by imprisonment for not more than a year and/or a fine of not more than $100,000 ($200,000 for an organization).[102]

---

[101] "(3) the term 'pen register' means a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached, but such term does not include any device used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business; (4) the term 'trap and trace device' means a device which captures the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted," 18 U.S.C. 3127(3),(4)). Although clone pagers are not considered pen registers, *Brown v. Waddell*, 50 F.3d 285, 290-91 (4th Cir. 1995), "caller id" services have been found to constitute trap and trace devices, *United States v. Fregoso*, 60 F.3d 1314, 1320 (8th Cir. 1995).

[102] "(a) In general – Except as provided in this section, no person may install or use a pen register or a trap and trace device without first obtaining a court order under section 3123 of this title or under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.).

"(b) Exception – The prohibition of subsection (a) does not apply with respect to the use of a pen register or a trap and trace device by a provider of electronic or wire communication service – (1) relating to the operation, maintenance, and testing of a wire or electronic communication service or to the protection of the rights or property of such provider, or to the protection of users of that service from abuse of service or unlawful use of service; or (2) to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire communication, or a user of that service, from fraudulent, unlawful or abusive use of service; or (3) where the consent of the user of that service has been obtained.

"(c) Limitation – A government agency authorized to install and use a pen register *or trap and trace device* under this chapter or under State law shall use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing, routing, addressing, and signaling information utilized in ~~call processing~~ identifying the origination or destination of wire or electronic communications. (d) Penalty.– Whoever knowingly violates subsection (a) shall be fined under this title or imprisoned not more than one year, or both," 18 U.S.C. 3121. The changes noted above are the work of the USA PATRIOT Act's expansion of the pen register/trap and trace provisions to embrace electronic communications, 115 Stat. 288-91 (2001); they are changes that do *not* sunset on

There is no accompanying exclusionary rule, however, and consequently a violation of section 3121 will serve as a basis to suppress any resulting evidence.[103]

Unlike other violations of Title III/ECPA, there is no separate federal private cause of action for victims of a pen register or trap and trace device violation. Some of the states have established a separate criminal offense for unlawful use of a pen register or trap and trace device, yet most of these do seem to follow the federal lead and decline to establish a separate private cause of action, *See* Appendix III.

Foreign Intelligence Surveillance Act

The Foreign Intelligence Surveillance Act (FISA) authorizes special court order in four purposes: electronic surveillance, physical searches, installation and use pen registers/trap and trace devices, and orders to disclose tangible items, 50 U.S.C. 1801-1861. The electronic surveillance portion of FISA, 50 U.S.C. 1801-1811, creates a procedure for judicially supervised "electronic surveillance" (wiretapping) conducted for foreign intelligence gathering purposes. The Act classifies four kinds of wiretapping as "electronic surveillance" and outlaws

- intentionally
- either
  - engaging in *electronic surveillance*
  - under color of law
  - except as authorized by statute, or

  - disclosing or using
  - information obtained under color of law
  - by *electronic surveillance*,
  - knowing or having reason to know
  - that the information was obtained by electronic surveillance not authorized by statute, 18 U.S.C. 1809.

The four classes of *electronic surveillance* involve wiretapping that could otherwise only be conducted under court order:

"(1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;

"(2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States, *does not include the acquisition of those communications of computer*

December 31, 2005, 115 Stat. 295 (2001).

[103] *United States v. Fregoso*, 60 F.3d 1314, 1320 (8th Cir. 1995); *United States v. Thompson*, 936 F.2d 1249, 1249-250 (11th Cir. 1991).

trespassers that would be permissible under section 2511(2)(i) of title 18, United States Code;

"(3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or

"(4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes," 50 U.S.C. 1801(f).[104]

The prohibitions apply only to federal officers and employees,[105] but do not apply to a law enforcement officer operating under a warrant or court.[106] Violations are punishable by imprisonment for not more than 5 years and/or a fine of not more than $250,000, *id.* and expose the offender to civil liability.[107] By virtue of USA PATRIOT Act amendments, victims of any improper use of information secured under a FISA surveillance order may also be entitled to actual or statutory damages.[108]

---

[104] The USA PATRIOT Act amended the definition of "electronic surveillance" so as to exclude interception of the electronic communications of a trespasser within the computer system of another thereby removing it from the prohibitions of section 1809, 115 Stat. 392 (2001). This is among the USA PATRIOT Act amendments that do *not* sunset on December 31, 2005, 115 Stat. 295 (2001).

[105] "There is Federal jurisdiction over an offense under this section if the person committing the offense was an officer or employee of the United States at the time the offense was committed," 50 U.S.C. 1809(d). For others, criminal proscriptions and exemptions of Title III (18 U.S.C. 2510-2518) would apply.

[106] "It is a defense to a prosecution under subsection (a) of this section that the defendant was a law enforcement or investigative officer engaged in the course of his official duties and the electronic surveillance was authorized by and conducted pursuant to a search warrant or court order of a court of competent jurisdiction," 50 U.S.C. 1809(d).

[107] "An aggrieved person, other than a foreign power or an agent of a foreign power, as defined in section 1801(a) or (b)(1)(A) of this title, respectively, who has been subjected to an electronic surveillance or about whom information obtained by electronic surveillance of such person has been disclosed or used in violation of section 1809 of this title shall have a cause of action against any person who committed such violation and shall be entitled to recover – (a) actual damages, but not less than liquidated damages of $1,000 or $100 per day for each day of violation, whichever is greater; (b) punitive damages; and (c) reasonable attorney's fees and other investigation and litigation costs reasonably incurred," 50 U.S.C. 1810. Victims are not entitled to injunctive relief, *ACLU Foundation of Southern California v. Barr*, 952 F.2d 457, 469-70 (D.C.Cir. 1992)(the court did not address the question of whether conduct in violation of both FISA and Title III/EPCA might be enjoined under 18 U.S.C. 2520(b)(1)).

[108] "Any person who is aggrieved by any willful violation of . . . section[] 106(a) . . . of the Foreign Intelligence Surveillance Act [relating to the use of information acquired from electronic surveillance under the Act] may commence an action in United States District Court against the United States to recover money damages. In any such action, if a person who is aggrieved successfully establishes a violation of . . . the above special provisions of

FISA also has its own exclusionary rule,[109] but Congress anticipated,[110] and the courts have acknowledged, that surveillance conducted under FISA for foreign

---

title 50, the Court may assess as damages – (1) actual damages, but not less than $10,000, whichever amount is greater; and (2) litigation costs, reasonably incurred," 18 U.S.C. 2712(a). This provision terminates on December 31, 2005, 115 Stat. 295 (2001).

[109] "If the United States district court pursuant to subsection (f) of this section determines that the surveillance was not lawfully authorized or conducted, it shall, in accordance with the requirements of law, suppress the evidence which was unlawfully obtained or derived from electronic surveillance of the aggrieved person or otherwise grant the motion of the aggrieved person. If the court determines that the surveillance was lawfully authorized and conducted, it shall deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure," 50 U.S.C. 1806(g).

"Whenever a court or other authority is notified pursuant to subsection (c) or (d) of this section, or whenever a motion is made pursuant to subsection (e) of this section, or whenever any motion or request is made by an aggrieved person pursuant to any other statute or rule of the United States or any State before any court or other authority of the United States or any State to discover or obtain applications or orders or other materials relating to electronic surveillance or to discover, obtain, or suppress evidence or information obtained or derived from electronic surveillance under this chapter, the United States district court or, where the motion is made before another authority, the United States district court in the same district as the authority, shall, notwithstanding any other law, if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States, review in camera and ex parte the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted. In making this determination, the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance," 50 U.S.C. 1806(f).

[110] S.REP.NO. 701, 95th Cong., 2d Sess. 61 (1978); 50 U.S.C. 1806(b)(". . . such information . . . may only be used in a criminal proceeding with the advance authorization of the Attorney General").

intelligence purposes may result in admissible evidence of a crime.[111]

The physical search portion of FISA authorizes the issuance of physical search orders for foreign intelligence gathering purposes, 50 U.S.C. 1821-1829. Its accompanying criminal proscriptions and civil liability provisions, and are identical to those used in the electronic surveillance portion of FISA.[112]

Procedure

Generally

Each of the prohibitions mentioned above recognizes a procedure for government use notwithstanding the general ban, usually under judicial supervision. Although Fourth Amendment concerns supply a common theme, the procedures are individually distinctive.

---

[111] When FISA required certification that the acquisition of foreign intelligence is formation was "the" purpose for seeking the a FISA surveillance order, there is some debate among the courts over how prominent the foreign intelligence purpose actually had to be, *United States v. Johnson*, 952 F.2d 565, 572 (1st Cir. 1992)("Although evidence obtained under FISA subsequently may be used in criminal prosecutions, the investigation of criminal activity cannot be the primary purpose of the surveillance"); *United States v. Duggan*, 743 F.2d 59, 77 (2d Cir. 1984)("The requirement that foreign intelligence information be the primary objective of the surveillance is plain. . ."); *United States v. Sarkissian*, 841 F.2d 959, 964 (9th Cir. 1988) ("Defendants rely on the primary purpose test . . . . We . . . decline to decide the issue. We have generally stated that the purpose of the surveillance must be to secure foreign intelligence information. . . . We refuse to draw too fine a distinction between criminal and intelligence investigations"); *United States v. Badia*, 827 F.2d 1458, 1463 (11th Cir. 1987)("An application for a FISA order must contain certification by a designated official of the executive branch that the purpose of the surveillance is to secure foreign intelligence information. . . . Once the certification is made, it is subjected to only minimal scrutiny by the courts"). The USA PATRIOT Act changed "the purpose" to "a significant purpose," a change which the FISA review court concluded demands only that the government have a "measurable" foreign intelligence purpose when it seeks a FISA surveillance order, *In re Sealed Case*, 310 F.3d 717, 734-35 (F.I.S.Ct.Rev. 2002). The language will revert to "the purpose" when the sunset provision takes effect after December 31, 2005.

[112] 50 U.S.C. 1827 ("A person is guilty of an offense if he intentionally – (1) under color of law for the purpose of obtaining foreign intelligence information, executes a physical search within the United States except as authorized by statute . . . ."); 50 U.S.C. 1828 ("An aggrieved person, other than a foreign power or an agent of a foreign power, as defined in section 1801(a) or (b)(1)(A), respectively, of this title, whose premises, property, information, or material has been subjected to a physical search within the United States or about whom information obtained by such a physical search has been disclosed or used in violation of section 1827 of this title shall have a cause of action against any person who committed such violation . . . ."); 18 U.S.C. 2712(a)("Any person who is aggrieved by any willful violation of . . . section[] 305(a) . . . of the Foreign Intelligence Surveillance Act [relating to the use of information acquired from a physical search under the Act] may commence an action in United States District Court against the United States to recover money damages. . . . ").

Law Enforcement Wiretapping and Electronic Eavesdropping

Title III/ECPA authorizes both federal and state law enforcement wiretapping and electronic eavesdropping, under court order, without the prior consent or knowledge of any of the participants, 18 U.S.C. 2516 - 2518. At the federal level, a senior Justice Department official must approve the application for the court order.[113] The procedure is only available where there is probable cause to believe that the wiretap or electronic eavesdropping will produce evidence of one of a long, but not exhaustive, list of federal crimes,[114] or of the whereabouts of a "fugitive from

---

[113] "The Attorney General, Deputy Attorney General, Associate Attorney General, or any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General or acting Deputy Assistant Attorney General in the Criminal Division specially designated by the Attorney General, may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant in conformity with section 2518 of this chapter an order authorizing or approving the interception of wire or oral communications by the Federal Bureau of Investigation, or a Federal agency having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of [the predicate offenses]. . ." 18 U.S.C. 2516(1).

[114] The predicate offense list includes conspiracy to violate or violations of: (1) 8 U.S.C. 1324 (smuggling aliens), 1327 (same), or 1328 (same); (2) bankruptcy fraud; (3) 18 U.S.C. §§32 (destruction of aircraft or their facilities), 33 (destruction of motor vehicles or their facilities), 38 (aircraft parts fraud), 115 (threatening or retaliating against federal officials), 175 (biological weapons), 201 (bribery of public officials and witnesses), 215 (bribery of bank officials), 224 (bribery in sporting contests), 229 (chemical weapons), 351 (assassinations, kidnapping, and assault of Members of Congress and certain other officials), 471-473 (counterfeiting), 659 (theft from interstate shipment), 664 (embezzlement from pension and welfare funds), 751 (escape), 791-798 (espionage and related felonies), 831 (traffic in nuclear materials), 844(d), (e), (f), (g), (h), or (i) (unlawful use of explosives), 892-894 (loansharking), 922 (firearms felonies), 924 (same), 1014 (bank fraud), 1028 (false identity felonies), 1029 (credit card fraud), 1030 (computer fraud and abuse), 1032 (bank fraud), 1084 (gambling), 1203 (hostage taking), 1341 (mail fraud), 1343 (wire fraud), 1344 (bank fraud), 1361-1367 (felonies relating to malicious mischief), 1425-1427 (immigration offenses), 1460-1470 (felonies relating to obscenity), 1503 (obstruction of justice), 1510-1513 (same), 1541-1546 (passport crimes), 1651-1661 (felonies relating to piracy), 1751 (assassination, kidnapping, and assault of the president and certain other executive officials), 1831-1839 (felonies related to trade secrets); 1951 (Hobbs Act), 1952 (Travel Act), 1954 (bribery relating to employee benefit plans), 1955 (gambling), 1956 (money laundering), 1957 (same), 1958 (murder for hire), 1959 (violence in aid of racketeering), 1963 (RICO), 1992 (wrecking trains), 2101-2102 (felonies relating to riots), 2151-2156 (sabotage and related felonies), 2251 and 2252 (sexual exploitation of children), 2271-2281 (felonies relating to shipping), 2312-2315 (interstate transportation of stolen property), 2321 (illicit trafficking in motor vehicles or motor vehicle parts), 2332 (violence against Americans overseas), 2332a (weapons of mass destruction), 2332b (terrorism transcending national borders), 2332d (financial transactions with terrorist supporting nations), 2339A (providing support to terrorists), 2339B (providing support to terrorist organizations), 2381-2390 (treason and related felonies), 2511-2512 (wiretapping felonies) 3146 (bail jumping), 3521(b)(3) (disclosing information relating to witness relocation), and any other provision of title 18 of the United States Code involving murder, kidnapping, robbery, or extortion;(4) drug trafficking; (5) 22 U.S.C. 2778 (Arms Export Control Act offenses); (6) 26 U.S.C. §5861 (firearms offenses); (7) 29 U.S.C. §§186 (corruption of labor unions), 501(c)(same),or murder, kidnaping, robbery or extortion if punishable under title 29; (8) 31 U.S.C. §5322

justice" fleeing from prosecution of one of the offenses on the predicate offense list, 18 U.S.C. 2516(1)(*l*). Any federal prosecutor may approve an application for a court order under section 2518 authorizing the interception of e-mail or other electronic communications during transmission.[115]

At the state level, the principal prosecuting attorney of a state or any of its political subdivisions may approve an application for an order authorizing wiretapping or electronic eavesdropping based upon probable cause to believe that it will produce evidence of a felony under the state laws covering murder, kidnaping, gambling, robbery, bribery, extortion, drug trafficking, or any other crime dangerous to life, limb or property. State applications, court orders and other procedures must at a minimum be as demanding as federal requirements.[116]

Applications for a court order authorizing wiretapping and electronic surveillance include:

- the identity of the applicant and the official who authorized the application;
- a full and complete statement of the facts including
  - details of the crime,
  - a particular description of nature, location and place where the interception is to occur,[117]

(money laundering); (9) 42 U.S.C. §§2274-2277 (felonies under the Atomic Energy Act); 2284 (felonies relating to sabotage at nuclear facilities); and (10) 49 U.S.C. §§60123(b) (destruction of a natural gas pipeline), 46502 (air piracy).

[115] "Any attorney for the Government (as such term is defined for the purposes of the Federal Rules of Criminal Procedure) may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant, in conformity with section 2518 of this title, an order authorizing or approving the interception of electronic communications by an investigative or law enforcement officer having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of any Federal felony," 18 U.S.C. 2516(3). The less demanding procedures of 18 U.S.C. 2701-2711 may be used with respect to e-mail or other electronic communications that are in storage; recourse to subsection 2516(3) is only necessary when on-going electronic communications are to be "intercepted."

[116] "The principal prosecuting attorney of any State, or the principal prosecuting attorney of any political subdivision thereof, if such attorney is authorized by a statute of that State to make application to a State court judge of competent jurisdiction for an order authorizing or approving the interception of wire, oral, or electronic communications, may apply to such judge for, and such judge may grant in conformity with section 2518 of this chapter and with the applicable State statute an order authorizing, or approving the interception of wire, oral, or electronic communications by investigative or law enforcement officers having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of the commission of the offense of murder, kidnapping, gambling, robbery, bribery, extortion, or dealing in narcotic drugs, marihuana or other dangerous drugs, or other crime dangerous to life, limb, or property, and punishable by imprisonment for more than one year, designated in any applicable State statute authorizing such interception, or any conspiracy to commit any of the foregoing offenses," 18 U.S.C. 2516(2).

[117] Requirements that may be excused under the circumstances provided in subsections (11) and (12) sometimes referred to as authorizing "roving wiretaps":

- a particular description of the communications to be intercepted, and
- the identities (if known) of the person committing the offense and of the persons whose communications are to be intercepted;

• a full and complete statement of the alternative investigative techniques used or an explanation of why they would be futile or dangerous;
• a statement of period of time for which the interception is to be maintained and if it will not terminate upon seizure of the communications sought, a probable cause demonstration that further similar communications are likely to occur;
• a full and complete history of previous interception applications or efforts involving the same parties or places;
• in the case of an extension, the results to date or explanation for the want of results; and
• any additional information the judge may require, 18 U.S.C. 2518(1), (2).

Before issuing an order authorizing interception, the court must find:

• probable cause to believe that an individual is, has or is about to commit one or more of the predicate offenses;
• probable cause to believe that the particular communications concerning the crime will be seized as a result of the interception requested;
• that normal investigative procedures have been or are likely to be futile or too dangerous; and
• probable cause to believe that "the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted are being

---

"The requirements of subsections (1)(b)(ii) and (3)(d) of this section relating to the specification of the facilities from which, or the place where, the communication is to be intercepted do not apply if – (a) in the case of an application with respect to the interception of an oral communication – (i) the application is by a Federal investigative or law enforcement officer and is approved by the Attorney General, the Deputy Attorney General, the Associate Attorney General, an Assistant Attorney General, or an acting Assistant Attorney General; (ii) the application contains a full and complete statement as to why such specification is not practical and identifies the person committing the offense and whose communications are to be intercepted; and (iii) the judge finds that such specification is not practical; and (b) in the case of an application with respect to a wire or electronic communication – (i) the application is by a Federal investigative or law enforcement officer and is approved by the Attorney General, the Deputy Attorney General, the Associate Attorney General, an Assistant Attorney General, or an acting Assistant Attorney General; (ii) the application identifies the person believed to be committing the offense and whose communications are to be intercepted and the applicant makes a showing of a purpose, on the part of that person, to thwart interception by changing facilities; and (iii) the judge finds that such purpose has been adequately shown.

"An interception of a communication under an order with respect to which the requirements of subsections (1)(b)(ii) and (3)(d) of this section do not apply by reason of subsection (11) shall not begin until the facilities from which, or the place where, the communication is to be intercepted is ascertained by the person implementing the interception order. A provider of wire or electronic communications service that has received an order as provided for in subsection (11)(b) may move the court to modify or quash the order on the ground that its assistance with respect to the interception cannot be performed in a timely or reasonable fashion. The court, upon notice to the government, shall decide such a motion expeditiously," 18 U.S.C. 2518(11), (12).

used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person," 18 U.S.C. 2518(3).

Subsections 2518(4) and (5) demand that any interception order include:

- the identity (if known) of the persons whose conversations are to be intercepted;
- the nature and location of facilities and place covered by the order;
- a particular description of the type of communication to be intercepted and an indication of the crime to which it relates;
- individual approving the application and the agency executing the order;
- the period of time during which the interception may be conducted and an indication of whether it may continue after the communication sought has been seized;
- an instruction that the order shall be executed
  - as soon as practicable, and
  - so as to minimize the extent of innocent communication seized; and
- upon request, a direction for the cooperation of communications providers and others necessary or useful for the execution of the order, 18 U.S.C. 2518(4).

Compliance with these procedures may be postponed until after the interception effort has begun, upon the approval of senior Justice Department officials in emergency cases involving organized crime or national security threatening conspiracies or involving the risk of death or serious injury, 18 U.S.C. 2718(7).[118]

The authority of the court orders extends only as long as required but not more than 30 days. After 30 days, the court may grant 30 day extensions subject to the procedures required for issuance of the original order, 18 U.S.C. 2518(5). During that time the court may require progress reports at such intervals as it considers appropriate, 18 U.S.C. 2518(6).

---

[118] "Notwithstanding any other provision of this chapter, any investigative or law enforcement officer, specially designated by the Attorney General, the Deputy Attorney General, the Associate Attorney General or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant to a statute of that State, who reasonably determines that – (a) an emergency situation exists that involves – (i) immediate danger of death or serious physical injury to any person, (ii) conspiratorial activities threatening the national security interest, or (iii) conspiratorial activities characteristic of organized crime – that requires a wire, oral, or electronic communication to be intercepted before an order authorizing such interception can, with due diligence, be obtained, and

"(b) there are grounds upon which an order could be entered under this chapter to authorize such interception, may intercept such wire, oral, or electronic communication if an application for an order approving the interception is made in accordance with this section within forty-eight hours after the interception has occurred, or begins to occur. In the absence of an order, such interception shall immediately terminate when the communication sought is obtained or when the application for the order is denied, whichever is earlier. In the event such application for approval is denied, or in any other case where the interception is terminated without an order having been issued, the contents of any wire, oral, or electronic communication intercepted shall be treated as having been obtained in violation of this chapter, and an inventory shall be served as provided for in subsection (d) of this section on the person named in the application," 18 U.S.C. 2518(7).

Intercepted communications are to be recorded and the evidence secured and placed under seal (with the possibility of copies for authorized law enforcement disclosure and use) along with the application and the court's order, 18 U.S.C. 2518(8)(a),(b).

Within 90 days of the expiration of the order those whose communications have been intercepted are entitled to notice, and evidence secured through the intercept may be introduced into evidence with 10 days advance notice to the parties, 18 U.S.C. 2518(8)(d), (9).

Title III also circumscribes the conditions under which information derived from a court ordered interception may be disclosed or otherwise used. It may be disclosed and used for official purposes to:

- other law enforcement officials[119] including foreign officials;[120]
- federal intelligence officers to the extent that it involves foreign intelligence information;[121]

---

[119] "(1) Any investigative or law enforcement officer who, by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents to another investigative or law enforcement officer to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure. (2) Any investigative or law enforcement officer who, by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication or evidence derived therefrom may use such contents to the extent such use is appropriate to the proper performance of his official duties . . . (5) When an investigative or law enforcement officer, while engaged in intercepting wire, oral, or electronic communications in the manner authorized herein, intercepts wire, oral, or electronic communications relating to offenses other than those specified in the order of authorization or approval, the contents thereof, and evidence derived therefrom, may be disclosed or used as provided in subsections (1) and (2) of this section. . . ." 18 U.S.C. 2517(1),(2),(5).

[120] *Any investigative or law enforcement officer, or other Federal official in carrying out official duties as such Federal official, who by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents or derivative evidence to a foreign investigative or law enforcement officer to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure, and foreign investigative or law enforcement officers may use or disclose such contents or derivative evidence to the extent such use or disclosure is appropriate to the proper performance of their official duties,*" 18 U.S.C. 2517(7). The Homeland Security Act added this subsection, 116 Stat. 2257 (2002).

[121] "*Any investigative or law enforcement officer, or attorney for the Government, who by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents to any Federal law enforcement, intelligence, protective, immigration, national defense, or national security official to the extent that such contents include foreign intelligence or counterintelligence (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 401a), or foreign intelligence information (as defined in subsection (19) of section 2510 of this title), to assist the official who is to receive that information in the performance of his official duties. Any Federal official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person's*

• other American or foreign government officials to the extent that it involves the threat of hostile acts by foreign powers, their agents, or international terrorists.[122]

---

official duties subject to any limitations on the unauthorized disclosure of such information," 18 U.S.C. 2517(6).

"'[F]oreign intelligence information', for purposes of section 2517(6) of this title, means – (A) information, whether or not concerning a United States person, that relates to the ability of the United States to protect against – (i) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; (ii) sabotage or intentional terrorism by a foreign power or an agent of a foreign power; or (iii) clandestine intelligence activities by and intelligence service or network of a foreign power or by an agent of a foreign power; or (B) information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to – (i) the national defense or the security of the United States; or (ii) the conduct of the foreign affairs of the United States," 18 U.S.C. 2510(19). The USA PATRIOT Act added subsections 2517(6) and 2510(19), 115 Stat. 280 (2001). The additions disappear when the USA PATRIOT Act sunset provisions go into effect, 115 Stat. 295 (2001).

[122] *Any investigative or law enforcement officer, or other Federal official in carrying out official duties as such Federal official, who by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents or derivative evidence to any appropriate Federal, State, local, or foreign government official to the extent that such contents or derivative evidence reveals a threat of actual or potential attack or other grave hostile acts of a foreign power of an agent of as foreign power, domestic or international sabotage, domestic or international terrorism, or clandestine intelligence gathering activities by an intelligence service or network of a foreign power or by an agent of a foreign power, within the United States or elsewhere, for the purpose of preventing or responding to such a threat. Any official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information, and any State, local, or foreign official who receives information pursuant to this provision may use that information only consistent with such guidelines as the Attorney General and Director of Central Intelligence shall jointly issue*, 18 U.S.C. 2517(8). The Homeland Security Act added this subsection, 116 Stat. 2257 (2002).

It may also be disclosed by witnesses testify in federal or state proceedings,[123] provided the intercepted conversation or other communication is not privileged.[124]

Stored Electronic or Wire Communications

The procedural requirements for law enforcement access to stored wire or electronic communications and transactional records are less demanding but equally complicated, 18 U.S.C. 2701-2712. They deal with two kinds of information – often in the custody of the telephone company or some other service provider rather than of any of the parties to the communication – the communications records and th content of electronic or wire communications. Law enforcement officials are entitled to access:

- with the consent of the one of the parties;[125]

- on the basis of a court order or similar process under the procedures established in Title III/ECPA;[126]

---

[123] "(3) Any person who has received, by any means authorized by this chapter, any information concerning a wire, oral, or electronic communication, or evidence derived therefrom intercepted in accordance with the provisions of this chapter may disclose the contents of that communication or such derivative evidence while giving testimony under oath or affirmation in any proceeding held under the authority of the United States or of any State or political subdivision thereof.. . . . (5) When an investigative or law enforcement officer, while engaged in intercepting wire, oral, or electronic communications in the manner authorized herein, intercepts wire, oral, or electronic communications relating to offenses other than those specified in the order of authorization or approval, the contents thereof, and evidence derived therefrom, may be disclosed or used as provided in subsections (1) and (2) of this section. Such contents and any evidence derived therefrom may be used under subsection (3) of this section when authorized or approved by a judge of competent jurisdiction where such judge finds on subsequent application that the contents were otherwise intercepted in accordance with the provisions of this chapter. Such application shall be made as soon as practicable," 18 U.S.C. 2517(3),(5).

[124] "No otherwise privileged wire, oral, or electronic communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character," 18 U.S.C. 2517(4).

[125] "(b) A provider described in subsection (a) may divulge the contents of a communication . . . (3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service. . . . (c) . . . A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service, (not including the contents of communications covered by subsection (a)(1) or (a)(2)) . . . (2) with the lawful consent of the customer or subscriber. " 18 U.S.C. 2702(b)(3),(c)(2).

[126] "A provider described in subsection (a) may divulge the contents of a communication . . . (2) as otherwise authorized in section 2517, 2511(2)(a), or 2703 . . . .(c) . . . A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service, (not including the contents of communications covered by subsection (a)(1) or (a)(2)) (1) as otherwise authorized in section 2703, " 18 U.S.C. 2702(b)(2), (c)(1).

• in certain emergency situations;[127] or

• under one of the other statutory exceptions to the ban on service provider disclosure.[128]

Section 2703, which affords law enforcement access to the content of stored wire and electronic communications, distinguishing between recent communications and those that have been in electronic storage for more than 6 months. Government officials may gain access to wire or electronic communications in electronic storage for less than 6 months under a search warrant issued upon probable cause to believe

---

[127] "(b) A provider described in subsection (a) may divulge the contents of a communication . . . (7) to a federal, state, or local governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency. (c) . . . A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service, (not including the contents of communications covered by subsection (a)(1) or (a)(2)) . . .(4) to a government entity, if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure of the information, 18 U.S.C. 2702(b)(7),(c)(4).

[128] "(b) A provider described in subsection (a) may divulge the contents of a communication – (1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient; . . . (4) to a person employed or authorized or whose facilities are used to forward such communication to its destination; (5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service; (6) to a law enforcement agency – (A) if the contents – (i) were inadvertently obtained by the service provider; and (ii) appear to pertain to the commission of a crime; (B) if required by section 227 of the Crime Control Act of 1990 (42 U.S.C. 13002) [relating to service provider obligations to report child pornography]. . . (c) . . . A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service, (not including the contents of communications covered by subsection (a)(1) or (a)(2)) . . . (3) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service," 18 U.S.C. 2702(b)(1),(4),(5),(6); (c)(3).

a crime has been committed and the search will produce evidence of the offense.[129]

The government must used the same procedure to acquire older communications or those stored in remote computer storage if access is to be afforded without notice to the subscriber or customer.[130] If government officials are willing to afford the subscriber or customer notice or at least delayed notice, access may be granted under a court order showing that the information sought is relevant and material to a criminal investigation or under an administrative subpoena, a grand jury subpoena, a trial subpoena, or court order.[131] Under the court order procedure, the court may

---

[129] 18 U.S.C. 2703(a)("A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a~~n~~ *wire or* electronic communication, that is in electronic storage in a~~n~~ *wire or* electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant. . . ."). The USA PATRIOT Act amendments reflected above allow access to voice mail under the procedures previously limited to e-mail and other electronic communications, 115 Stat. 283 (2001); the coverage disappears when the USA PATRIOT Act's sunset provision takes effect after December 31, 2005, 115 Stat. 295 (2001). The 21st Century Department of Justice Appropriations Authorization Act, 116 Stat. 1822 (2002), amended section 2703 to permit execution of the warrant by service providers and others without requiring the presence of a federal officer, 18 U.S.C. 2703(g)("Notwithstanding section 3105 of this title, the presence of an officer shall not be required for service or execution of a search warrant issued in accordance with this chapter requiring disclosure by a provider of electronic communications service or remote computing service of the contents of communications or records or other information pertaining to a subscriber to or customer of such service"), see *United States v. Bach*, 310 F.3d 1063 (8th Cir. 2002)(the Fourth Amendment does not require the presence of a federal officer when technicians execute a search warrant on a service provider's server).

[130] "(a) . . . A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a~~n~~ *wire or* electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

"(b)(1) A governmental entity may require a provider of remote computing service to disclose the contents of any *wire or* electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection – (A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation . . . (2) Paragraph (1) is applicable with respect to any *wire or* electronic communication that is held or maintained on that service – (A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and (B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing," 18 U.S.C. 2703(a), (b)(1)(A), (2).

[131] "(b)(1) A governmental entity may require a provider of remote computing service to disclose the contents of any *wire or* electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection . . .(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity – (i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or (ii) obtains a court order for such disclosure under subsection (d)

authorize delayed notification 90 day increments in cases where contemporaneous notice might have an adverse impact.[132] Government supervisor officials may certify the need for delayed notification in the case of a subpoena.[133] Traditional exigent circumstances and a final general inconvenience justification form the grounds for delayed notification in either case:

- endangering the life or physical safety of an individual;
- flight from prosecution;
- destruction of or tampering with evidence;
- intimidation of potential witnesses; or
- otherwise seriously jeopardizing an investigation or unduly delaying a trial, 18 U.S.C. 2705(a)(2), (b).

Comparable, if less demanding, procedures apply when the government seeks other customer information from a service provider (other than the content of a customer's communications). The information can be secured:

- with a warrant;
- with a court order;
- with customer consent;
- with a written request in telemarketing fraud cases; or

---

of this section; except that delayed notice may be given pursuant to section 2705 of this title . . . .(d) A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider," 18 U.S.C. 2703(b)(1)(B), (d).

[132] "(1) A governmental entity acting under section 2703(b) of this title may – (A) where a court order is sought, include in the application a request, which the court shall grant, for an order delaying the notification required under section 2703(b) of this title for a period not to exceed ninety days, if the court determines that there is reason to believe that notification of the existence of the court order may have an adverse result described in paragraph (2) of this subsection . . . (4) Extensions of the delay of notification provided in section 2703 of up to ninety days each may be granted by the court upon application . . . but only in accordance with subsection (b) of this section," 18 U.S.C. 2705(a)(1)(A), (4).

[133] "(1) A governmental entity acting under section 2703(b) of this title may . . . (B) where an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury subpoena is obtained, delay the notification required under section 2703(b) of this title for a period not to exceed ninety days upon the execution of a written certification of a supervisory official that there is reason to believe that notification of the existence of the subpoena may have an adverse result described in paragraph (2) of this subsection. . . (4) Extensions of the delay of notification provided in section 2703 of up to ninety days each may be granted . . . by certification by a governmental entity, but only in accordance with subsection (b) of this section," 18 U.S.C. 2705(a)(1)(B), (4).

• with a subpoena in some instances.[134]

Most customer identification, use, and billing information can be secured simply with a subpoena and without customer notification.[135]

Pen Registers and Trap and Trace Devices

Pen registers and trap and trace devices identify the source of calls placed to or from a particular telephone. Federal government attorneys and state and local police officers may apply for a court order authorizing the installation and use of a pen register and/or a trap and trace device upon certification that the information that will provide is relevant to a pending criminal investigation, 18 U.S.C. 3122.[136]

---

[134] "(1) A government entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) – (A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant; (B) obtains a court order for such disclosure under subsection (d) of this section; (C) has the consent of the subscriber or customer to such disclosure; or (D) submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section 2325 of this title); or (E) seeks information under paragraph (2) . . . (3) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer," 18 U.S.C. 2703(c)(1),(3).

[135] "(2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the (A) name; (B) address; (C) local and long distance telephone connection records, or records of session times and durations; (D) length of service (including start date) and types of service utilized; (E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and (F) means and source of payment (including any credit car or bank account number), of a subscriber to or customer of such service, when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1). (3) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer," 18 U.S.C. 2703(c)(2),(3). Although not noted here or above, the USA PATRIOT Act rewrote subsection 2703(c), 115 Stat. 283, 285 (2001). The changes in paragraph 2703(c)(2) are *not* among those that sunset after December 31, 2005, 115 Stat. 295 (2001).

[136] "(a)(1) An attorney for the Government may make application for an order or an extension of an order under section 3123 of this title authorizing or approving the installation and use of a pen register or a trap and trace device under this chapter, in writing under oath or equivalent affirmation, to a court of competent jurisdiction. (2) Unless prohibited by State law, a State investigative or law enforcement officer may make application for an order or an extension of an order under section 3123 of this title authorizing or approving the installation and use of a pen register or a trap and trace device under this chapter, in writing under oath or equivalent affirmation, to a court of competent jurisdiction of such State.

"(b) An application under subsection (a) of this section shall include – (1) the identity of the attorney for the Government or the State law enforcement or investigative officer making the application and the identity of the law enforcement agency conducting the investigation; and (2) a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency,"

An order authorizing installation and use of a pen register or trap and trace device must:

- specify
  - the person (if known) upon whose telephone line the device is to be installed,
  - the person (if known) who is the subject of the criminal investigation,
  - the telephone number, (if known) the location of the line to which the device is to be attached, and geographical range of the device,
  - a description of the crime to which the investigation relates;
- upon request, direct carrier assistance pursuant to section 3124;[137]
- terminate within 60 days, unless extended;

---

18 U.S.C. 3122.

[137] "(a) Upon the request of an attorney for the Government or an officer of a law enforcement agency authorized to install and use a pen register under this chapter, a provider of wire or electronic communication service, landlord, custodian, or other person shall furnish such investigative or law enforcement officer forthwith all information, facilities, and technical assistance necessary to accomplish the installation of the pen register unobtrusively and with a minimum of interference with the services that the person so ordered by the court accords the party with respect to whom the installation and use is to take place, if such assistance is directed by a court order as provided in section 3123(b)(2) of this title.

"(b) Upon the request of an attorney for the Government or an officer of a law enforcement agency authorized to receive the results of a trap and trace device under this chapter, a provider of a wire or electronic communication service, landlord, custodian, or other person shall install such device forthwith on the appropriate line *or other facility* and shall furnish such investigative or law enforcement officer all additional information, facilities and technical assistance including installation and operation of the device unobtrusively and with a minimum of interference with the services that the person so ordered by the court accords the party with respect to whom the installation and use is to take place, if such installation and assistance is directed by a court order as provided in section 3123(b)(2) of this title. Unless otherwise ordered by the court, the results of the trap and trace device shall be furnished, pursuant to section 3123(b) or section 3125 of this title, to the officer of a law enforcement agency, designated in the court order, at reasonable intervals during regular business hours for the duration of the order.

"(c) A provider of a wire or electronic communication service, landlord, custodian, or other person who furnishes facilities or technical assistance pursuant to this section shall be reasonably compensated for such reasonable expenses incurred in providing such facilities and assistance.

"(d) No cause of action shall lie in any court against any provider of a wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with a court order under this chapter or request pursuant to section 3125 of this title.

"(e) A good faith reliance on a court order under this chapter, a request pursuant to section 3125 of this title, a legislative authorization, or a statutory authorization is a complete defense against any civil or criminal action brought under this chapter or any other law.

"(f) Pursuant to section 2522, an order may be issued to enforce the assistance capability and capacity requirements under the Communications Assistance for Law Enforcement Act," 18 U.S.C. 3124 (emphasis added). The USA PATRIOT Act supplied the language italicized above to reflect the fact that it authorized the use of pen register and trap and trace orders in connection with computer as well as telephone communications, 115 Stat. 290 (2001). The change is *not* among those that expire after December 31, 2005, 115 Stat. 295 (2001).

- involve a report of particulars of the order's execution in Internet cases; and
- impose necessary nondisclosure requirements, 18 U.S.C. 3123.[138]

---

[138] "(a)(1) Upon a [federal] application made under section 3122(a)(1) of this title, the court shall enter an ex parte order authorizing the installation and use of a pen register or a trap and trace device if the court finds, based on facts contained in the application, that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation. Such order shall, upon service of such order, apply to any entity providing wire or electronic communication service in the United States whose assistance may facilitate the execution of the order. . . .be obtained by such installation and use is relevant to an ongoing criminal investigation. (3)(A) Where the law enforcement agency implementing an ex part order under this subsection seeks to do so by installing and using its own pen register or trap and trace device on a packet-switched data network of a provider of electronic communication service to the public the agency shall ensure that a record will be maintained which will identify – (i) any officer or officers who installed the device and any officer or officers who accessed the device to obtain information from the network; (ii) the date and time the device was installed, the date and time the device was uninstalled, and the date, time, and duration of each time the device is accessed to obtain information; (iii) the configuration of the device at the time of its installation and any subsequent modification thereof; and (iv) any information which has been collected by the device. To the extent that the pen register or trap and trace device can be set automatically to record this information electronically, the record shall be maintained electronically throughout the installation and use of the such device. (B) The record maintained under subparagraph (A) shall be provided ex parte and under seal to the court which entered the ex parte order authorizing the installation and use of the device within 30 days after termination of the order (including any extensions thereof).

"(b) An order issued under this section – (1) shall specify – (A) the identity, if known, of the person to whom is leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied; (B) the identity, if known, of the person who is the subject of the criminal investigation; (C) the attributes of the communications to which the order applies, including the number or other identifier and, if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied, and, in the case of an order authorizing installation and use of a trap and trace device under subsection (a)(2), the geographic limits of the order; and (D) a statement of the offense to which the information likely to be obtained by the pen register or trap and trace device relates; and (2) shall direct, upon the request of the applicant, the furnishing of information, facilities, and technical assistance necessary to accomplish the installation of the pen register or trap and trace device under section 3124 of this title.

"(c)(1) An order issued under this section shall authorize the installation and use of a pen register or a trap and trace device for a period not to exceed sixty days. (2) Extensions of such an order may be granted, but only upon an application for an order under section 3122 of this title and upon the judicial finding required by subsection (a) of this section. The period of extension shall be for a period not to exceed sixty days.

"(d) An order authorizing or approving the installation and use of a pen register or a trap and trace device shall direct that – (1) the order be sealed until otherwise ordered by the court; and (2) the person owning or leasing the line or other facility to which the pen register or a trap and trace device is attached, or applied, or who is obligated by the order to provide assistance to the applicant, not disclose the existence of the pen register or trap and trace device or the existence of the investigation to the listed subscriber, or to any other person, unless or until otherwise ordered by the court," 18 U.S.C. 3123. Although not specifically noted above, the USA PATRIOT Act amended this section to make it applicable to electronic as well as wire communications, 115 Stat. 289-90 (2001). The amendments are *not* among those that expire after December 31, 2005, 115 Stat. 295 (2001).

Senior Justice Department or state prosecutors may approve the installation and use of a pen register or trap and trace device prior to the issuance of court authorization in emergency cases that involving either an organized crime conspiracy, an immediate danger of death or serious injury, an threat to national security, or a serious attack on a "protected computer," 18 U.S.C. 3125.[139]

Foreign Intelligence Surveillance Act

The procedure for securing wiretapping court orders under the Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. 1801-1811, is the most distinctive of the wiretap-related procedures.[140] First, it's focus is different. It is designed to secure foreign intelligence information not evidence of a crime. Second, it operates in a highly secretive manner. But its most individualistic feature is that the

---

[139] "(a) Notwithstanding any other provision of this chapter, any investigative or law enforcement officer, specially designated by the Attorney General, the Deputy Attorney General, the Associate Attorney General, any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General, or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant to a statute of that State, who reasonably determines that – (1) an emergency situation exists that involves – (A) immediate danger of death or serious bodily injury to any person; (B) conspiratorial activities characteristic of organized crime; *(C) an immediate threat to a national security interest; or (D) an ongoing attack on a protected computer (as defined in section 1030)* that constitutes a crime punishable by a term of imprisonment greater than one year; that requires the installation and use of a pen register or a trap and trace device before an order authorizing such installation and use can, with due diligence, be obtained, and (2) there are grounds upon which an order could be entered under this chapter to authorize such installation and use; may have installed and use a pen register or trap and trace device if, within forty-eight hours after the installation has occurred, or begins to occur, an order approving the installation or use is issued in accordance with section 3123 of this title.

"(b) In the absence of an authorizing order, such use shall immediately terminate when the information sought is obtained, when the application for the order is denied or when forty-eight hours have lapsed since the installation of the pen register or trap and trace device, whichever is earlier.

"(c) The knowing installation or use by any investigative or law enforcement officer of a pen register or trap and trace device pursuant to subsection (a) without application for the authorizing order within forty-eight hours of the installation shall constitute a violation of this chapter.

"(d) A provider of a wire or electronic service, landlord, custodian, or other person who furnished facilities or technical assistance pursuant to this section shall be reasonably compensated for such reasonable expenses incurred in providing such facilities and assistance," 18 U.S.C. 3125(emphasis added). The Homeland Security Act extended the grounds for emergency installation to include national security threats and serious attacks on protected computers, 116 Stat. 2158 (2002); H.Rep.No. 107-497, at 16-7 (2002). A "protected computer" is "a computer – (A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or (B) which is used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States," 18 U.S.C. 1030(e)(2).

[140] *See generally*, Bazan, *The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework*, CRS REP.NO. RL30465 (2002).

procedure is conducted entirely before members of an independent court convened for no other purpose. The Act operates in the field of foreign intelligence gathering, primarily through a Foreign Intelligence Surveillance Court whose judges grant or reject petitions for wiretap and electronic surveillance orders, orders authorizing physical searches and seizures, pen register and trap and trace orders, and orders to the surrender of tangible items.

The Foreign Intelligence Surveillance Court is comprised of eleven federal court judges designated by the Chief Justice to sit on the Court for a single seven year term, 50 U.S.C. 1803(a),(b),(d).[141] In the area of wiretaps and physical searches,[142] the judges of the Court individually receive and approve or reject requests, authorized by the Attorney General, to conduct four specific types of

---

[141] "(a) Court to hear applications and grant orders; record of denial; transmittal to court of review – The Chief Justice of the United States shall publicly designate ~~seven~~ *11* district court judges from seven of the United States judicial circuits *of whom no fewer than 3 shall reside within 20 miles of the District of Columbia* who shall constitute a court which shall have jurisdiction to hear applications for and grant orders approving electronic surveillance anywhere within the United States under the procedures set forth in this chapter, except that no judge designated under this subsection shall hear the same application for electronic surveillance under this chapter which has been denied previously by another judge designated under this subsection. If any judge so designated denies an application for an order authorizing electronic surveillance under this chapter, such judge shall provide immediately for the record a written statement of each reason for his decision and, on motion of the United States, the record shall be transmitted, under seal, to the court of review established in subsection (b) of this section transmitted under seal, to the court of review established in subsection (b) of this section.

"(b) Court of review; record, transmittal to Supreme Court – The Chief Justice shall publicly designate three judges, one of whom shall be publicly designated as the presiding judge, from the United States district courts or courts of appeals who together shall comprise a court of review which shall have jurisdiction to review the denial of any application made under this chapter. If such court determines that the application was properly denied, the court shall immediately provide for the record a written statement of each reason for its decision and, on petition of the United States for a writ of certiorari, the record shall be transmitted under seal to the Supreme Court, which shall have jurisdiction to review such decision.

* * *

"(d) Tenure – Each judge designated under this section shall so serve for a maximum of seven years and shall not be eligible for redesignation, except that the judges first designated under subsection (a) of this section shall be designated for terms of from one to seven years so that one term expires each year, and that judges first designated under subsection (b) of this section shall be designated for terms of three, five, and seven years," 50 U.S.C. 1803(a),(b),(d). The USA PATRIOT Act increased the size of the FISA court from 7 to 11 and required that at 3 members of the court live within 20 miles of Washington, 115 Stat. 283 (2001). These changes are permanent and do *not* expire after December 31, 2005, 115 Stat. 295 (2001).

[142] The FISA procedures relating to wiretapping and electronic surveillance orders, 50 U.S.C. 1801-1811, and those relating to physical searches, 50 U.S.C. 1821-1829, are virtually identical and consequently are treated together here.

wiretapping (electronic surveillance)[143] in order to intercept the communications of foreign powers.

The contents of FISA application include:

- the identity of the individual submitting the application;
- an indication of the President's grant of authority and the approval of the Attorney General or a Deputy Attorney General;
- the identity or a description of the person whose communications are to be intercepted;
- an indication of
  - why the person is believed to be a foreign power or the agent of a foreign power,[144] and

---

[143] "'Electronic surveillance,' means – (1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;

"(2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States, *does not include the acquisition of those communications of computer trespassers that would be permissible under section 2511(2)(i) of title 18, United States Code*;

"(3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or

"(4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes," 50 U.S.C. 1801(f)(emphasis added). The USA PATRIOT Act added the permanent language italicize above, 115 Stat. 392, 295 (2001). There is no definition of "electronic surveillance" in the FISA physical search provisions, cf., 50 U.S.C. 1821 (relating to definitions used in 50 U.S.C. 1821-1829).

The courts have noted that, unlike surveillance under Title III/EPCA, silent video surveillance falls within the purview of FISA by virtue of subsection 1801(1)(4), *United States v. Koyomejian*, 970 F.2d 536, 540 (9th Cir. 1992); *United States v. Mesa-Rincon*, 911 F.2d 1433, 1438 (10th Cir. 1990); *United States v. Biasucci*, 786 F.2d 504, 508 (2d Cir. 1986).

[144] "'Foreign power' means – (1) a foreign government or any component thereof, whether or not recognized by the United States; (2) a faction of a foreign nation or nations, not substantially composed of United States persons; (3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments; (4) a group engaged in international terrorism or activities in preparation therefor; (5) a foreign-based political organization, not substantially composed of United States persons; or (6) an entity that is directed and controlled by a foreign government or governments.

"'Agent of a foreign power' means – (1) any person other than a United States person, who – (A) acts in the United States as an officer or employee of a foreign power, or as a

- why foreign powers or their agents are believed to use the targeted facilities or places;
• a summary of the minimization procedures[145] to be followed;
• a detailed description of the communications to be intercepted and the information sought;

---

member of a foreign power as defined in subsection (a)(4) of this section; (B) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person's presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities; or (2) any person who – (A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States; (B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States; (C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, or on behalf of a foreign power; or (D) knowingly aids or abets any person in the conduct of activities described in subparagraph (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraph (A), (B), or (C)," 50 U.S.C. 1801(a),(b). The FISA physical search provisions adopt by cross reference these definitions of "foreign power" and "agent of a foreign power," 50 U.S.C. 1821(1).

Note that the definition of foreign power includes international terrorists groups regardless of whether any nexus to a foreign power can be shown, 50 U.S.C. 1801(a)(4) and includes agents of foreign powers that no longer exist, *United States v. Squillacote*, 221 F.3d 542, 554 (4th Cir. 2000)(agents of East Germany intercepted under an order granted after unification).

[145] "'Minimization procedures', with respect to electronic surveillance, means – (1) specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;

"(2) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in subsection (e)(1) of this section, shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance;

"(3) notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes; and

"(4) notwithstanding paragraphs (1), (2), and (3), with respect to any electronic surveillance approved pursuant to section 1802(a) of this title, procedures that require that no contents of any communication to which a United States person is a party shall be disclosed, disseminated, or used for any purpose or retained for longer than ~~twenty-four~~ *72* hours unless a court order under section 1805 of this title is obtained or unless the Attorney General determines that the information indicates a threat of death or serious bodily harm to any person," 50 U.S.C. 1801(h). The definition for physical search purposes is the same except references to physical searches rather than electronic surveillance, 50 U.S.C. 1821(4). The Intelligence Authorization Act for Fiscal Year 2002, P.L. 107-108, extended the permissible duration of emergency orders from 24 to 72 hours as noted above and under section 1821(4)(D), 115 Stat. 1402 (2001).

• certification by a senior national security or senior defense adviser to the President that

- the information sought is foreign intelligence information,

- *a significant* purpose of interception is to secure foreign intelligence information,[146]

- the information cannot reasonably be obtained using alternative means,

• the means of accomplishing the interception (including whether a physical entry will be required);

• a history of past interception applications involving the same persons, places or facilities;

• the period of time during which the interception is to occur, whether it will terminate immediately upon obtaining the information sought, and if not, the reasons why interception thereafter is likely to be productive;

• whether more than one interception device is to be used and if so their range and the minimization procedures associated with each (only if the target is a foreign agent; if the target is a foreign power, an indication of the communications of and information about Americans likely to be intercepted).50 U.S.C. 1804.[147]

FISA court judges issue orders approving electronic surveillance or physical searches upon a finding that the application requirements have been met and that there is probable cause to believe that the target is a foreign power or the agent of a foreign power and that the targeted places or facilities are used by foreign powers of their agents.[148]

---

[146] The USA PATRIOT Act changed the language from "the purpose" to "a significant purpose," under both the surveillance and physical search requirements, 115 Stat. 291 (2001). The FISA Court of Review subsequently held that the change permitted application for a FISA surveillance order when authorities "have a measurable foreign intelligence purpose, other than just criminal prosecution of even foreign intelligence crimes," *In re Sealed Case*, 310 F.3d 717, 735 (F.I.S.Ct.Rev. 2002). The "the purpose" language returns when the USA PATRIOT Act amendment sunsets after December 31, 2005, 115 Stat. 295 (2001).

[147] 50 U.S.C. 1823 relating applications for a FISA physical search order is essentially the same.

[148] "Upon an application made pursuant to section 1804 of this title, the judge shall enter an ex parte order as requested or as modified approving the electronic surveillance if he finds that – (1) the President has authorized the Attorney General to approve applications for electronic surveillance for foreign intelligence information; (2) the application has been made by a Federal officer and approved by the Attorney General; (3) on the basis of the facts submitted by the applicant there is probable cause to believe that – (A) the target of the electronic surveillance is a foreign power or an agent of a foreign power: Provided, That no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States; and (B) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power; (4) the proposed minimization procedures meet the definition of minimization procedures under section 1801(h) of this title; and (5) the application which has been filed contains all statements and certifications required by section 1804 of this title and, if the target is a United States person, the certification or certifications are not clearly erroneous on the basis of the statement made under section 1804(a)(7)(E) of this title and any other information furnished under section 1804(d) of this title," 50 U.S.C. 1805(a); see, 1824(a)(to

Orders approving electronic surveillance or physical searches must:

• specify
- the identity or a description of the person whose communications are to be intercepted,
- the nature and location of the targeted facilities or places, *if known*,[149]
- type of communications or activities targeted and the kind of information sought,
- the means by which interception is to be accomplished and whether physical entry is authorized,[150]
- the tenure of the authorization, and
- whether more than one device are to be used and if so their respective ranges and associated minimization procedures;[151]
• require
- that minimization procedures be adhered to,
- upon request, that carriers and others provide assistance,[152]
- that those providing assistance observe certain security precautions, and be compensated;[153]

---

the same effect with respect to physical searches rather than electronic surveillance).

[149] This "if known" language, added by the Intelligence Authorization Act for Fiscal Year 2002, 115 Stat. 1402 (2001), contemplates "roving" wiretaps and has no physical search counterpart.

[150] The issue of whether physical entry will be necessary to execute the order, raised in subsections 1805(c) and (d), is only relevant in the case of surveillance orders which may often be executed without entry onto the premises of the target; there is no physical search companion requirement.

[151] This requirement has no mate in the physical search section, see, 18 U.S.C. 1824(c)(1).

[152] "An order approving an electronic surveillance under this section shall . . . (2) direct – (B) that, upon the request of the applicant, a specified communication or other common carrier, landlord, custodian, or other specified person , *or in circumstances where the Court finds that the actions of the target of the application may have the effect of thwarting the identification of a specified person, such other persons,* furnish the applicant forthwith all information, facilities, or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy and produce a minimum of interference with the services that such carrier, landlord, custodian, or other person is providing that target of electronic surveillance," 50 U.S.C. 1805(c)(2)(B); see, 50 U.S.C. 1824(c)(2)(b), but here too in language supplied by the USA PATRIOT Act, 115 Stat. 282 (2001) the electronic surveillance section alone contemplates the possibility of roving wiretaps in cases where the target attempts thwart surveillance. The distinction will disappear after December 31, 2005 when the USA PATRIOT Act authority for such roving surveillance sunsets, 115 Stat. 295 (2001).

[153] "An order approving an electronic surveillance under this section shall. . . (2) direct. . . (C) that such carrier, landlord, custodian, or other person maintain under security procedures approved by the Attorney General and the Director of Central Intelligence any records concerning the surveillance or the aid furnished that such person wishes to retain; and (D) that the applicant compensate, at the prevailing rate, such carrier, landlord, custodian, or other person for furnishing such aid," 50 U.S.C. 1805(c)(2)(C),(D); see, 50 U.S.C. 1824(c)(2)(C),(D). Only the physical search order must also insist that "the federal officer conducting the physical search promptly report to the court the circumstances and results of the physical search," 50 U.S.C. 1824(c)(2)(E).

• expire when its purpose is accomplished but not later than after 90 days generally (after 120 days in the case of foreign agents and after a year in the case of foreign governments or their entities or factions of foreign nations) unless extended (extensions may not exceed 1 year), 50 U.S.C. 1805(c).[154]

As in the case of law enforcement wiretapping and electronic eavesdropping, there is authority for interception and physical searches prior to approval in emergency situations, 50 U.S.C. 1805(e),[155] but there is also statutory authority for foreign intelligence surveillance interceptions and physical searches without the

---

The USA PATRIOT Act's amendments make it clear that those who provide such assistance are immune from civil suit, 18 U.S.C. 1805(i)(" No cause of action shall lie in any court against any provider of a wire or electronic communication service, landlord, custodian, or other persons (including any officer, employee, agent, or other specified person thereof) that furnishes any information, facilities, or technical assistance in accordance with a court order or request for emergency assistance under this Act for electronic surveillance or physical search"). Note that the USA PATRIOT Act amendment here disappears after December 31, 2005, 115 Stat. 295 (2001).

[154] 18 U.S.C. 1824(c) (relating to physical search orders) is essentially the same. The USA PATRIOT Act increased the tenure of orders relating to foreign agents to 120 days in both instances and establish a common general duration of 90 days for both, 115 Stat. 282 (2001), amendments that sunset after December 31, 2005 (2001).

[155] "Notwithstanding any other provision of this subchapter, when the Attorney General reasonably determines that – (1) an emergency situation exists with respect to the employment of electronic surveillance to obtain foreign intelligence information before an order authorizing such surveillance can with due diligence be obtained; and (2) the factual basis for issuance of an order under this subchapter to approve such surveillance exists – he may authorize the emergency employment of electronic surveillance if a judge having jurisdiction under section 1803 of this title is informed by the Attorney General or his designee at the time of such authorization that the decision has been made to employ emergency electronic surveillance and if an application in accordance with this subchapter is made to that judge as soon as practicable, but not more than ~~twenty-four~~ *72* hours after the Attorney General authorizes such surveillance. If the Attorney General authorizes such emergency employment of electronic surveillance, he shall require that the minimization procedures required by this subchapter for the issuance of a judicial order be followed. In the absence of a judicial order approving such electronic surveillance, the surveillance shall terminate when the information sought is obtained, when the application for the order is denied, or after the expiration of ~~twenty-four~~ *72* hours from the time of authorization by the Attorney General, whichever is earliest. In the event that such application for approval is denied, or in any other case where the electronic surveillance is terminated and no order is issued approving the surveillance, no information obtained or evidence derived from such surveillance shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any United States person acquired from such surveillance shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of such person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person. A denial of the application made under this subsection may be reviewed as provided in section 1803 of this title," 50 U.S.C. 1805(f); see also, 50 U.S.C. 1824(e). The Intelligence Authorization Act for Fiscal Year 2002, P.L. 107-108, extended the permissible duration of emergency orders from 24 to 72 hours in both instances as noted above, 115 Stat. 1402 (2001).

requirement of a court order when the targets are limited to communications among or between foreign powers or involve nonverbal communications from places under the open and exclusive control of a foreign power, 50 U.S.C. 1802(a)(1),(4).[156] The second of these is replete with reporting requirements to Congress and the FISA court, 50 U.S.C. 1802(a)(2),(3).[157] These and the twin war time exceptions[158] may

---

[156] "(1) Notwithstanding any other law, the President, through the Attorney General, may authorize electronic surveillance without a court order under this subchapter to acquire foreign intelligence information for periods of up to one year if the Attorney General certifies in writing under oath that – (A) the electronic surveillance is solely directed at – (i) the acquisition of the contents of communications transmitted by means of communications used exclusively between or among foreign powers, as defined in section 1801(a)(1), (2), or (3) of this title; or (ii) the acquisition of technical intelligence, other than the spoken communications of individuals, from property or premises under the open and exclusive control of a foreign power, as defined in section 1801(a)(1), (2), or (3) of this title; (B) there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party; and (C) the proposed minimization procedures with respect to such surveillance meet the definition of minimization procedures under section 1801(h) of this title; and – if the Attorney General reports such minimization procedures and any changes thereto to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence at least thirty days prior to their effective date, unless the Attorney General determines immediate action is required and notifies the committees immediately of such minimization procedures and the reason for their becoming effective immediately. . . .

"(4) With respect to electronic surveillance authorized by this subsection, the Attorney General may direct a specified communication common carrier to -- (A) furnish all information, facilities, or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy and produce a minimum of interference with the services that such carrier is providing its customers; and (B) maintain under security procedures approved by the Attorney General and the Director of Central Intelligence any records concerning the surveillance or the aid furnished which such carrier wishes to retain – The Government shall compensate, at the prevailing rate, such carrier for furnishing such aid," 50 U.S.C. 1802(a)(1),(4); see, 50 U.S.C. 1822(a)(1), (4) for parallel physical search language.

[157]"(2) An electronic surveillance authorized by this subsection may be conducted only in accordance with the Attorney General's certification and the minimization procedures adopted by him. The Attorney General shall assess compliance with such procedures and shall report such assessments to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence under the provisions of section 1808(a) of this title.

"(3) The Attorney General shall immediately transmit under seal to the court established under section 1803(a) of this title a copy of his certification. Such certification shall be maintained under security measures established by the Chief Justice with the concurrence of the Attorney General, in consultation with the Director of Central Intelligence, and shall remain sealed unless – (A) an application for a court order with respect to the surveillance is made under sections 1801(h)(4) and 1804 of this title; or (B) the certification is necessary to determine the legality of the surveillance under section 1806(f) of this title," 50 U.S.C. 1802(a)(2),(3); see, 50 U.S.C. 1822(a)(2),(3) for physical search counterpart.

[158] "Notwithstanding any other law, the President, through the Attorney General, may authorize electronic surveillance without a court order under this subchapter to acquire foreign intelligence information for a period not to exceed fifteen calendar days following a declaration of war by the Congress, " 50 U.S.C. 1811.

"Notwithstanding any other provision of law, the President, through the Attorney

be subject to constitutional limitations, particularly when Americans are the surveillance targets.[159]

FISA has detailed provisions governing the use of the information acquired through the use of its surveillance or physical search authority that include:

- confidentiality requirements;[160]
- notice of required Attorney General approval for disclosure;[161]
- notice to the "aggrieved" of the government's intention to use the results as evidence;[162]

General, may authorize physical searches without a court order under this subchapter to acquire foreign intelligence information for a period not to exceed 15 calendar days following a declaration of war by the Congress," 50 U.S.C. 1829.

[159] *United States v. Bin Laden*, 126 F.Supp.2d 264, 281-82 (S.D.N.Y. 2000)(overseas surveillance of an American (who was an international terrorist) found contrary to Fourth Amendment requirements). *United States v. United States District Court (Keith)*, 407 U.S. 297, 321-22 (1972), held that the Fourth Amendment does not permit warrantless electronic surveillance of domestic terrorists, but left open "the issues which may be involved with respect to activities of foreign powers or their agents."

[160] "Information acquired from an electronic surveillance conducted pursuant to this subchapter concerning any United States person may be used and disclosed by Federal officers and employees without the consent of the United States person only in accordance with the minimization procedures required by this subchapter. No otherwise privileged communication obtained in accordance with, or in violation of, the provisions of this subchapter shall lose its privileged character. No information acquired from an electronic surveillance pursuant to this subchapter may be used or disclosed by Federal officers or employees except for lawful purposes," 50 U.S.C. 1806(a); see also, 50 U.S.C. 1825(a) (relating to physical searches).

[161] "No information acquired pursuant to this subchapter shall be disclosed for law enforcement purposes unless such disclosure is accompanied by a statement that such information, or any information derived therefrom, may only be used in a criminal proceeding with the advance authorization of the Attorney General," 50 U.S.C. 1806(b); see also, 50 U.S.C. 1825(c)(relating to physical searches).

[162] "Whenever the Government intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, against an aggrieved person, any information obtained or derived from an electronic surveillance of that aggrieved person pursuant to the authority of this subchapter, the Government shall, prior to the trial, hearing, or other proceeding or at a reasonable time prior to an effort to so disclose or so use that information or submit it in evidence, notify the aggrieved person and the court or other authority in which the information is to be disclosed or used that the Government intends to so disclose or so use such information.

"Whenever any State or political subdivision thereof intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of a State or a political subdivision thereof, against an aggrieved person any information obtained or derived from an electronic surveillance of that aggrieved person pursuant to the authority of this subchapter, the State or political subdivision thereof shall notify the aggrieved person, the court or other authority in which the information is to be disclosed or used, and the Attorney General that the State or political subdivision thereof intends to so disclose or so use such information," 50 U.S.C. 1806(c),(d); see also, 50 U.S.C. 1825(d), (e).

- suppression procedures;[163]
- dealing with inadvertently captured information;[164]

---

[163] "Any person against whom evidence obtained or derived from an electronic surveillance to which he is an aggrieved person is to be, or has been, introduced or otherwise used or disclosed in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the evidence obtained or derived from such electronic surveillance on the grounds that – (1) the information was unlawfully acquired; or (2) the surveillance was not made in conformity with an order of authorization or approval. Such a motion shall be made before the trial, hearing, or other proceeding unless there was no opportunity to make such a motion or the person was not aware of the grounds of the motion.

"Whenever a court or other authority is notified pursuant to subsection (c) or (d) of this section, or whenever a motion is made pursuant to subsection (e) of this section, or whenever any motion or request is made by an aggrieved person pursuant to any other statute or rule of the United States or any State before any court or other authority of the United States or any State to discover or obtain applications or orders or other materials relating to electronic surveillance or to discover, obtain, or suppress evidence or information obtained or derived from electronic surveillance under this chapter, the United States district court or, where the motion is made before another authority, the United States district court in the same district as the authority, shall, notwithstanding any other law, if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States, review in camera and ex parte the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted. In making this determination, the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance.

"If the United States district court pursuant to subsection (f) of this section determines that the surveillance was not lawfully authorized or conducted, it shall, in accordance with the requirements of law, suppress the evidence which was unlawfully obtained or derived from electronic surveillance of the aggrieved person or otherwise grant the motion of the aggrieved person. If the court determines that the surveillance was lawfully authorized and conducted, it shall deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure.

"Orders granting motions or requests under subsection (g) of this section, decisions under this section that electronic surveillance was not lawfully authorized or conducted, and orders of the United States district court requiring review or granting disclosure of applications, orders, or other materials relating to a surveillance shall be final orders and binding upon all courts of the United States and the several States except a United States court of appeals and the Supreme Court," 50 U.S.C. 1806(e),(f),(g),(h); see also, 1825(f),(g),(h),(i).

[164] "In circumstances involving the unintentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States, such contents shall be destroyed upon recognition, unless the Attorney General determines that the contents indicate a threat of death or serious bodily harm to any person." 50 U.S.C. 1806(i). The related physical search section is a little different, 50 U.S.C. 1825(b)("Where a physical search authorized and conducted pursuant to section 1824 of this title involves the residence of a United States person, and, at any time after the search the Attorney General determines there is no national

• notification emergency surveillance or search for which no FISA order was subsequently secured;[165] and
• clarification that those who execute FISA surveillance or physical search orders may consult with federal and state law enforcement officers.[166]

Pen Registers and Trap and Trace Devices.

FISA pen register and trap and trace procedures, 50 U.S.C. 1841-1846, are similar to those of their law enforcement counterparts, but with many of the attributes of other FISA provisions. The orders may be issued either by a member of the FISA court or by a FISA magistrate upon the certification of a federal officer that the information sought is likely to be relevant to an investigation of international terrorism or clandestine intelligence activities, 50 U.S.C. 1842.[167] They allow the Attorney General to authorize emergency installation and use as long as an application is filed within 48 hours, 50 U.S.C. 1843, and restrict the use of any

---

security interest in continuing to maintain the secrecy of the search, the Attorney shall provide notice to the United States person whose residence was searched of the fact of the search conducted pursuant to this chapter and shall identify any property of such person seized, altered, or reproduced during such search").

[165] "If an emergency employment of electronic surveillance is authorized under section 1805(e) of this title and a subsequent order approving the surveillance is not obtained, the judge shall cause to be served on any United States person named in the application and on such other United States persons subject to electronic surveillance as the judge may determine in his discretion it is in the interest of justice to serve, notice of – (1) the fact of the application; (2) the period of the surveillance; and (3) the fact that during the period information was or was not obtained. On an ex parte showing of good cause to the judge the serving of the notice required by this subsection may be postponed or suspended for a period not to exceed ninety days. Thereafter, on a further ex parte showing of good cause, the court shall forego ordering the serving of the notice required under this subsection," 50 U.S.C. 1806(j); see also, 50 U.S.C. 1825(j).

[166] "Federal officers who conduct electronic surveillance to acquire foreign intelligence information under this title may consult with Federal law enforcement officers or law enforcement personnel of a State or political subdivision of a State (including the chief executive officer of that State or political subdivision who has the authority to appoint or direct the chief law enforcement officer of that State or political subdivision to coordinate efforts to investigate or protect against – (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; (B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power. (2) Coordination authorized under paragraph (1) shall not preclude the certification required by section 104(a)(7)(B)[relating to the required certification that foreign intelligence gathering is a "significant purpose" for the FISA application] or the entry of an order under section 105," 50 U.S.C. 1806(k); see also, 50 U.S.C. 1825(k). The USA PATRIOT Act added subsection 1806(k) and 1825(k), 115 Stat. 364-65 (2001), the additions will remain in effect even after others have expired after December 31, 2005, 115 Stat. 295 (2001)..

[167] The USA PATRIOT Act expanded them to cover both wire and electronic communications and eliminated the additional certification requirement that the related communications concern clandestine intelligence or international terrorist activities or involve individuals engaged in such activities, 115 Stat. 286-87 (2001), changes that disappear after December 31, 2005, 115 Stat. 295 (2001).

resulting evidence if an order is not subsequently granted.[168] The provisions for use of the information acquired run parallel to those that apply to FISA surveillance and physical search orders, 50 U.S.C. 1845.

Tangible Items.

FISA's tangible items orders, 50 U.S.C. 1861, are perhaps its most interesting feature. Prior to the USA PATRIOT Act senior FBI officials could approve an application to a FISA judge or magistrate for an order authorizing common carriers, or public accommodation, storage facility, or vehicle rental establishments to release their business records based upon certification of a reason to believe that the records pertained to a foreign power or the agent of a foreign power, 50 U.S.C. 1862(2000 ed.). The USA PATRIOT Act rewrote the procedure. In its current form, it requires rather than authorizes disclosure; it makes no mention of probable cause, reason to believe, or relevancy; it applies to all tangible property not merely records; it applies to the tangible property of both individuals or organizations, commercial and otherwise.[169] It is limited, however, to investigations conducted to secure foreign

---

[168] "In the event that an application for an order applied for under subsection (a)(2) is denied, or in any other case where the installation and use of a pen register or trap and trace device under this section is terminated and no order under section 1842(b)(2) of this title is issued approving the installation and use of the pen register or trap and trace device, as the case may be, no information obtained or evidence derived from the use of the pen register or trap and trace device, as the case may be, shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any United States person acquired from the use of the pen register or trap and trace device, as the case may be, shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of such person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person," 50 U.S.C. 1843(c)(2).

[169] "(a)(1) The Director of the Federal Bureau of Investigation or a designee of the Director (whose rank shall be no lower than Assistant Special Agent in Charge) may make an application for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States persons or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution. (2) An investigation conducted under this section shall – (A) be conducted under guidelines the Attorney General under Executive Order No. 12333 (or a successor order); and (B) not be conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

"(b) Each application under this section – (1) shall be made to – (A) a judge of the court established by section 103(a); or (B) a United States Magistrate Judge under chapter 43 of Title 28 [28 U.S.C. s 631 et seq.], who is publicly designated by the Chief Justice of the United States to have the power to hear applications and grant orders for the production of tangible things under this section on behalf of a judge of that court; and (2) shall specify that the records concerned are sought for an authorized investigation conducted in accordance with subsection (a)(2) this section to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities.

"(c)(1) Upon application made pursuant to this section, the judge shall enter an ex parte

intelligence information or to protect against international terrorism or clandestine intelligence activities. Taken at face value, it seems to build upon the assumption that federal investigations of purely foreign activities in this country, even when the evidence is held by someone other than foreign national, are per se reasonable for Fourth Amendment purposes.[170]

---

order as requested, or as modified, approving the release of records if the judge finds that the application satisfies the requirements of this section. (2) An order under this subsection shall not disclose that it is issued for purposes of an investigation described in subsection (a).

"(d) No person shall disclose to any person (other than those persons necessary to produce the tangible things under this section) that the Federal Bureau of Investigation has sought or obtained tangible things under this section.

"(e) A person who, in good faith, produces tangible things under a subpoena issued pursuant to this section shall not be liable to any other person for such production. Such production shall not be deemed to constitute a waiver of any privilege in any other proceeding or context," 50 U.S.C. 1861. The tangible item provisions expire after December 31, 2005, 115 Stat. 295 (2001).

[170] Consider, *In re Sealed Case*, 310 F.3d 717, 746 (F.I.S.Ct.Rev. 2002)("Even without taking into account the President's inherent constitutional authority to conduct warrantless foreign intelligence surveillance, we think the procedures and government showings required under FISA, if they do not meet the minimum Fourth Amendment standards certainly come close. We, therefore, believe . . . that FISA as amended is constitutional because the surveillances it authorizes are reasonable").

Appendices

Appendix I. State Statutes Outlawing the Interception of Wire(w), Oral(o) and Electronic Communications(e)

Alabama: Ala.Code §§13A-11-30 to 13A-11-37(w/o);
Alaska: Alaska Stat. §§42.20.300 to 42.20.390(w/o/e);
Arizona: Ariz.Rev.Stat.Ann. §§13-3001 to 13-3009(w/o/e);
Arkansas: Ark.Code §5-60-120(w/o/e);
California: Cal.Penal Code §§631(w), 632(o), 632.7(e);

Colorado: Colo.Rev.Stat. §§18-9-301 to 18-9-305(w/o/e);
Connecticut: Conn.Gen.Stat.Ann. §§53a-187 to 53a-189(w/o);
Delaware: Del.Code tit.11 §2402(w/o/e);
Florida: Fla.Stat.Ann. §934.03(w/o/e);
Georgia: Ga.Code §16-11-62 (w/o/e);
Hawaii: Hawaii Rev.Stat. §§803-41, 803-42(w/o/e);
Idaho: Idaho Code §18-6702(w/o);

Illinois: Ill.Comp.Stat.Ann. ch.720 §5/14-2(w/o/e);
Indiana: Ind.Code Ann. §35-33.5-5-5(w/e);
Iowa: Iowa Code Ann. §808B.2(w/o/e);
Kansas: Kan.Stat.Ann. §21-4001(w/o); 21-4002(w);
Kentucky: Ky.Rev.Stat. §§526.010, 526.020(w/o);
Louisiana: La.Rev.Stat.Ann. §15:1303(w/o/e);

Maine: Me.Rev.Stat.Ann. ch.15 §§710(w/o);
Maryland: Md.Cts. & Jud.Pro.Code Ann. §10-402(w/o/e);
Massachusetts: Mass.Gen.Laws Ann. ch.272 §99(w/o);
Michigan: Mich.Comp.Laws Ann. §§750.539c(o); 750.540(w);
Minnesota: Minn.Stat.Ann. §626A.02(w/o/e);
Mississippi: Miss.Code §41-29-533(w/o/e)
Missouri: Mo.Ann.Stat. §542.402 (w/o);
Montana: Mont.Code Ann. §45-8-213(w/o/e);
Nebraska: Neb.Rev.Stat. §86-702(w/o);
Nevada: Nev.Rev.Stat. §§200.620(w), 200.650(o);
New Hampshire: N.H.Rev.Stat.Ann. §570-A:2 (w/o);

New Jersey: N.J.Stat.Ann. §2A:156A-3(w/o);
New Mexico: N.M.Stat.Ann. §30-12-1(w);
New York: N.Y.Penal Law §250.05(w/o/e);
North Carolina: N.C.Gen.Stat. §15A-287(w/o/e);
North Dakota: N.D.Cent.Code §§12.1-15-02 (w/o);
Ohio: Ohio Rev.Code §2933.52 (w/o/e);
Oklahoma: Okla.Stat.Ann. tit.13 §176.3 (w/o/e);
Oregon: Ore.Rev.Stat. §§165.535 to 165.545 (w/o/e);

Pennsylvania: Pa.Stat.Ann. tit.18 §5703 (w/o/e);
Rhode Island: R.I.Gen.Laws §§11-35-21(w/o/e);
South Dakota: S.D.Cod.Laws §23A-35A-20 (w/o);
Tennessee: Tenn.Code Ann. §39-13-601(w/o/e);
Texas: Tex.Penal Code. §§16.01 to 16.04 (w/o/e);
Utah: Utah Code Ann. §§77-23a-4, 77-23b-2 to 77-23b-4(w/o/e);

Virginia: Va.Code §19.2-62(w/o/e);
Washington: Wash.Rev.Code Ann. §9.73.030(w/o);
West Virginia: W.Va.Code §62-1D-3(w/o/e);
Wisconsin: Wis.Stat.Ann. §968.31(w/o/e);
Wyoming: Wyo.Stat. §7-3-702(w/o/e);
District of Columbia: D.C.Code §23-542(w/o).

Appendix II. Consent Interceptions Under State Law

Alabama: Ala.Code §13A-11-30 (one party consent);
Alaska: Alaska Stat. §§42.20.310, 42.20.330 (one party consent);
Arizona: Ariz.Rev.Stat.Ann. §13-3005 (one party consent);
Arkansas: Ark.Code §5-60-120 (one party consent);
California: Cal. Penal Code §§ 631, 632 (one party consent for police; all party consent otherwise);
Colorado: Colo.Rev.Stat. §§18-9-303, 18-9-304 (one party consent);
Connecticut: Conn.Gen.Stat.Ann. §§53a-187(one party consent);
Delaware: Del.Code tit.11 §2402 (one party consent);
Florida: Fla.Stat.Ann. §934.03 (one party consent for the police, all party consent for others);
Georgia: Ga.Code §16-11-66 (one party consent);
Hawaii: Hawaii Rev.Stat. §803-42 (one party consent);
Idaho: Idaho Code §18-6702 (one party consent);
Illinois: Ill.Comp.Stat.Ann. ch.720 §§5/14-2, 5/14-3 (all party consent with law enforcement exceptions);
Indiana: Ind.Code Ann. §35-33.5-1-5 (one party consent);
Iowa: Iowa Code Ann. §808B.2 (one party consent);
Kansas: Kan.Stat.Ann. §§21-4001, 21-4002 (all party consent);
Kentucky: Ky.Rev.Stat. §526.010 (one party consent);
Louisiana: La.Rev.Stat.Ann. §15:1303 (one party consent);
Maine: Me.Rev.Stat.Ann. ch.15 §§709, 712 (one party consent);
Maryland: Md.Cts. & Jud.Pro.Code Ann. §10-402 (all party consent);
Massachusetts: Mass.Gen.Laws Ann. ch.272 §99 (all parties must consent, except in some law enforcement cases);
Michigan: Mich.Comp.Laws Ann. §750.539c (eavesdropping proscriptions do not apply to otherwise lawful activities of peace officers);
Minnesota: Minn.Stat.Ann. §626A.02 (one party consent);
Mississippi: Miss.Code §41-29-531 (one party consent);
Missouri: Mo.Ann.Stat. §542.402 (one party consent);
Montana: Mont.Code Ann. §§45-8-213 (all party consent with an exception for the performance of official duties);
Nebraska: Neb.Rev.Stat. §86-702 (one party consent);
Nevada: Nev.Rev.Stat. §§200.620, 200.650 (one party consent);
New Hampshire: N.H.Rev.Stat.Ann. §570-A:2 (all party consent);
New Jersey: N.J.Stat.Ann. §§2A:156A-4 (one party consent);
New Mexico: N.M.Stat.Ann. §§30-12-1 (one party consent);
New York: N.Y.Penal Law §250.00 (one party consent);
North Carolina: N.C.Gen.Stat. §15A-287 (one party consent);
North Dakota: N.D.Cent.Code §§12.1-15-02 (one party consent);
Ohio: Ohio Rev.Code §2933.52 (one party consent);
Oklahoma: Okla.Stat.Ann. tit.13 §176.4 (one party consent);
Oregon: Ore.Rev.Stat. §165.540 (one party consent for wiretapping and all parties must consent for other forms of electronic eavesdropping);
Pennsylvania: Pa.Stat.Ann. tit.18 §5704 (one party consent for the police; all parties consent otherwise);
Rhode Island: R.I.Gen.Laws §§11-35-21 (one party consent);
South Dakota: S.D.Comp.Laws §§23A-35A-20 (one party consent);
Tennessee: Tenn.Code Ann. §39-13-601 (one party consent)
Texas: Tex.Penal Code §16.02 (one party consent);
Utah: Utah Code Ann. §§77-23a-4 (one party consent);
Virginia: Va.Code §19.2-62 (one party consent);

Washington: Wash.Rev.Code Ann. §9.73.030 (all parties must consent except in certain law enforcement cases);
West Virginia: W.Va.Code §62-1D-3 (one party consent);
Wisconsin: Wis.Stat.Ann. §968.31 (one party consent); **Wyoming**: Wyo.Stat. §7-3-702 (one party consent);
District of Columbia: D.C.Code §23-542 (one party consent).

Appendix III. Statutory Civil Liability for Interceptions Under State Law

Arizona: Ariz.Rev.Stat.Ann. §12-731;
California: Cal. Penal Code §§ 637.2;
Colorado: Colo.Rev.Stat. §18-9-309.5;
Connecticut: Conn.Gen.Stat.Ann. §54-41r;
Delaware: Del.Code tit.11 §2409;
Florida: Fla.Stat.Ann. §§934.10, 934.27;
Hawaii: Hawaii Rev.Stat. §803-48;
Idaho: Idaho Code §18-6709;
Illinois: Ill.Comp.Stat.Ann. ch.720 §5/14-6;
Indiana: Ind.Code Ann. §35-33.5-5-4;
Iowa: Iowa Code Ann. §808B.8;
Kansas: Kan.Stat.Ann. §22-2518
Louisiana: La.Rev.Stat.Ann. §15:1312;
Maine: Me.Rev.Stat.Ann. ch.15 §711;
Maryland: Md.Cts. & Jud.Pro.Code Ann. §§10-410, 10-4A-08;
Massachusetts: Mass.Gen.Laws Ann. ch.272 §99;
Michigan: Mich.Comp.Laws Ann. §750.539h;
Minnesota: Minn.Stat.Ann. §§626A.02, 626A.13;
Nebraska: Neb.Rev.Stat. §§86-707.2, 86-707.15;
Nevada: Nev.Rev.Stat. §200.690;
New Hampshire: N.H.Rev.Stat.Ann. §570-A:11;
New Jersey: N.J.Stat.Ann. §§2A:156-24;
New Mexico: N.M.Stat.Ann. §§30-12-11;
North Carolina: N.C.Gen.Stat. §15A-296;
Ohio: Ohio Rev.Code §2933.65;
Oregon: Ore.Rev.Stat. §133.739;
Pennsylvania: Pa.Stat.Ann. tit.18 §§5725, 5747;
Rhode Island: R.I.Gen.Laws §12-5.1-13;
Tennessee: Tenn.Code Ann. §39-13-603;
Texas: Tex.Code Crim.Pro. §18.20;
Utah: Utah Code Ann. §§77-23a-11; 77-23b-8;
Virginia: Va.Code §19.2-69;
Washington: Wash.Rev.Code Ann. §9.73.060;
West Virginia: W.Va.Code §62-1D-12;
Wisconsin: Wis.Stat.Ann. §968.31;
Wyoming: Wyo.Stat. §7-3-710;
District of Columbia: D.C.Code §23-554.

Appendix IV. Court Authorized Interception Under State Law

Alaska: Alaska Stats. §§12.37.010 to 12.37.900;
Arizona: Ariz.Rev.Stat.Ann. §§13-3010 to 13-3017;
California: Cal.Penal Code §629 to 629.98;
Colorado: Colo.Rev.Stat. §§16-15-101 to 16-15-104;
Connecticut: Conn.Gen.Stat.Ann. §§54-41a to 54-41t;
Delaware: Del.Code tit.11 §§2401 to 2412;
Florida: Fla.Stat.Ann. §§934.02 to 934.43;
Georgia: Ga.Code §16-11-64;
Hawaii: Hawaii Rev.Stat. §§803-41 to 803-49;
Idaho: Idaho Code §§18-6701 to 18-6725;
Illinois: Ill.Stat.Ann. ch.725 §§5/108A-1 to 108B-14;
Indiana:Ind.Code §§35-33.5-1-1 to 35-33.5-5-6;
Iowa: Iowa Code Ann. §§808B.3 to 808B.7;
Kansas: Kan.Stat.Ann. §§22-2401 to 22-2414;
Louisiana: La.Rev.Stat.Ann. §§15:1301 to 15:1316;
Maryland: Md.Cts. & Jud.Pro.Code Ann. §§10-401 to 10-410;
Massachusetts: Mass.Gen.Laws Ann. ch.272 §99;
Minnesota: Minn.Stat.Ann. §§626A.01 to 626.41;
Mississippi: Miss.Code §§41-29-501 to 41-29-537;
Missouri: Mo.Ann.Stat. §§542.400 to 542.424;
Nebraska: Neb.Rev.Stat. §§86-701 to 86-712;
Nevada: Nev.Rev.Stat. §§179.410 to 179.515;
New Hampshire: N.H.Rev.Stat.Ann. §§570-A:1 to 570-A:9;
New Jersey: N.J.Stat.Ann. §§2A:156A-8 to 2A:156A-26;
New Mexico: N.M.Stat.Ann. §§30-12-1 to 30-12-14;
New York: N.Y.Crime.Pro. Law §§700.05 to 700.70;
North Carolina: N.C.Gen.Stat. §§15A-286 to 15A-298;
North Dakota: N.D.Cent.Code §§29-29.2-01 to 29-29.2-05;
Ohio: Ohio Rev.Code §§2933.51 to 2933.66;
Oklahoma: Okla.Stat.Ann. tit.13 §§176.1 to 176.14
Oregon: Ore.Rev.Stat. §§133.721 to 133.739;
Pennsylvania: Pa.Stat.Ann. tit.18 §§5701 to 5728
Rhode Island: R.I.Gen.Laws §§12-5.1-1 to 12-5.1-16;
South Dakota: S.D.Cod.Laws §§23A-35A-1 to 23A-35A-34
Tennessee: Tenn.Code Ann. §§40-6-301 to 40-6-311;
Texas: Tex.Crim.Pro. Code. §18.20;
Utah: Utah Code Ann. §§77-23a-1 to 77-23a-16;
Virginia: Va.Code §§19.2-61 to 19.2-70.3;
Washington: Wash.Rev.Code Ann. §§9.73.040 to 9.73.250;
West Virginia: W.Va.Code §§62-1D-1 to 62-1D-16;
Wisconsin: Wis.Stat.Ann. §§968.27 to 968.33;
Wyoming: Wyo.Stat. §§7-3-701 to 7-3-712;
District of Columbia: D.C.Code §§23-541 to 23-556.

Appendix V. State Statutes Regulating Stored Electronic Communications (SE), Pen Registers (PR) and Trap and Trace Devices (T)

Alaska: Alaska Stats. §§12.37.200 (PR&T), 12.37.300(SE);
Arizona: Ariz.Rev.Stat.Ann. §§13-3016 (SE), 13-3017 (PR&T);
Delaware: Del.Code tit.11 §§2421 to 2426 (SE), 2430 to 2434 (PR&T);
Florida: Fla.Stat.Ann. §§934.21 to 934.28 (SE); 934.32 to 934.34(PR&T);
Georgia: Ga.Code Ann. §§16-11-60 to 16-11-64.2 (PR &T);
Hawaii: Hawaii Rev.Stat. §§803-44.5, 803-44.6 (PR&T), 803-47.5 to 803.47.9 (SE);
Idaho: Idaho Code §§18-6721 to 18-6723 (PR&T);
Iowa: Iowa Code Ann. §§808B.10 to 808B.14;
Kansas: Kan.Stat.Ann. §§22-2525 to 22-2529 (PR&T);
Louisiana: La.Rev.Stat.Ann. §§15:1313 to 15:1316 (PR&T);
Maryland: Md.Cts. & Jud.Pro.Code Ann. §§10-4A-01 to 10-4A-08 (SE), 10-4B-01 to 10-4B-05 (PR&T);
Minnesota: Minn.Stat.Ann. §§626A.24 to (SE), 626A.35 to 636A.391 (PR&T);
Mississippi: Miss.Code §41-29-701(PR&T);
Missouri: Mo.Ann.Stat. §542.408 (PR);
Montana: Mont.Code Ann. §§46-4-401 to 46-4-405 (PR&T);
Nebraska: Neb.Rev.Stat. §§86-707.3 to 86-707.07 (PR&T), 86-707.09 to 86-707.14 (SE);
Nevada: Nev.Rev.Stat. §§179.530 (PR&T), 205.492 to 205.513(SE);
New Hampshire: N.H.Rev.Stat.Ann. §§570-B:1 to 570-B:7 (PR&T);
New Jersey; N.J.Stat.Ann. §§2A:156A-27 to 2A:156A-34 (SE);
New York: N.Y.Crim.Pro.Law §§705.00 to 705.35 (PR&T);
North Carolina: N.C.Gen.Stat. §§15A-260 to 15A-264 (PR&T);
North Dakota: N.D.Cent.Code §§29-29.3-01 to 29-29.3-05 (PR&T);
Ohio: Ohio Rev.Code §2933.76 (PR&T);
Oklahoma: Okla.Stat.Ann. tit.13 §177.1 to 177.5 (PR&T);
Oregon: Ore.Rev.Stat. §§165.657 to 165.659 (PR&T);
Pennsylvania: Pa.Stat.Ann. tit.18 §§5741 to 5748 (SE), 5771 to 5775 (PR&T);
Rhode Island; R.I.Gen.Laws §§12-5.2-1 to 12-5.2-5 (PR&T);
South Carolina: S.C.Code §§17-29-10 to 17-29-50 (PR&T);
South Dakota: S.D.Cod.Laws §§23A-35A-22 to 23A-35A-34 (PR&T);
Tennessee: Tenn.Code Ann. §40-6-311 (PR&T);
Texas: Tex.Code of Crim.Pro. art. 18.21 (SE, PR&T);
Utah: Utah Code Ann. §§77-23a-14 (PR&T), 77-23b-2 to 77-23b-9(SE);
Virginia: Va.Code §§19.2-70.2 (PR&T), 19.2-70.3 (SE);
Washington: Wash.Rev.Code Ann. §9.73.260 (PR&T);
West Virginia: W.Va.Code §62-1D-10 (PR&T);
Wisconsin: Wis.Stat.Ann. §968.30 to 968.37 (PR&T);
Wyoming: Wyo.Stat. §§7-3-801 to 7-3-806 (PR&T).

Appendix VI. State Computer Crime Statutes

Alabama: Ala.Code §§13A-8-100 to 13A-8-103;
Alaska: Alaska Stat. §11.46.740;
Arizona: Ariz.Rev.Stat.Ann. §§13-2316 to 13-2316.02;
Arkansas: Ark.Code §§5-41-101 to 5-41-108;
California: Cal.Penal Code §§501, 502;
Colorado: Colo.Rev.Stat. §§18-5.5-101, 18-5.5-102;
Connecticut: Conn.Gen.Stat.Ann. §§53a-250 to 53a-261;
Delaware: Del.Code tit.11 §§931 to 939;
Florida: Fla.Stat.Ann. §§815.01 to 815.07;
Georgia: Ga.Code §§16-9-92 to 16-9-64;
Hawaii: Hawaii Rev.Stat. §708-890 to 708-896;
Idaho: Idaho Code §§18-2201, 18-2202;
Illinois: Ill.Stat.Ann. ch.720 §§5/16D-1 to 5/16D-7;
Indiana: Ind.Code §§35-43-1-4 to 35-43-2-3;
Iowa: Iowa Code Ann. §716.6B;
Kansas: Kan.Stat.Ann. §21-3755;
Kentucky: Ky.Rev.Stat. §§434.840 to 434.860;
Louisiana: La.Rev.Stat.Ann. §§14:73.1 to 14:73.5;
Maine: Me.Rev.Stat.Ann. ch.17-A §§431 to 433;
Maryland: Md.Code Ann. art. 27 §146;
Massachusetts: Mass.Gen.Laws Ann. ch.266 §120F;
Michigan: Mich.Comp.Laws Ann. §§752.791 to 752.797;
Minnesota: Minn.Stat.Ann. §§609.87 to 609.893;
Mississippi: Miss.Code §§97-45-1 to 97-45-13;
Missouri: Mo.Ann.Stat. §§569.093 to 569.099;
Montana: Mont.Code Ann. §§45-6-310, 45-6-311;
Nebraska: Neb.Rev.Stat. §§28-1341 to 28-1348;
Nevada: Nev.Rev.Stat. §§205.473 to 205.492;
New Hampshire: N.H.Rev.Stat.Ann. §638:16 to 638:19;
New Jersey: N.J.Stat.Ann. §§2C:20-23 to 2C:20-33;
New Mexico: N.M.Stat.Ann. §§30-20-1 to 30-20-7;
New York: N.Y.Penal Law §§156.00 to 156.50;
North Carolina: N.C.Gen.Stat. §§14-453 to 14-458;
North Dakota: N.D.Cent.Code §12.1-06.1-08;
Ohio: Ohio Rev.Code §§2913.01 to 2913.42;
Oklahoma: Okla.Stat.Ann. tit.21 §§1951 to 1958;
Oregon: Ore.Rev.Stat. §164.371;
Pennsylvania: Pa.Stat.Ann. tit.18 §3933;
Rhode Island: R.I.Gen.Laws §§11-52-1 to 11-52-8;
South Carolina: S.C.Code §§16-16-10 to 16-16-40;
South Dakota: S.D.Cod.Laws §§43-43B-1 to 43-43B-8;
Tennessee: Tenn.Code Ann. §§39-14-601 to 39-14-603;
Texas: Tex.Penal Code. §§33.01 to 33.03;
Utah: Utah Code Ann. §§76-6-702 to 76-6-705;
Virginia: Va.Code §§18.2-152.1 to 18.2-152.14;
Washington: Wash.Rev.Code Ann. §§9A.52.110 to 9A.52.130;
West Virginia: W.Va.Code §§61-3C-1 to 61-3C-21;
Wisconsin: Wis.Stat.Ann. §943.70;
Wyoming: Wyo.Stat. §§6-3-501 to 6-3-504.

Selected Bibliography

Books & Articles

Abramovsky, *Surreptitious Recording of Witnesses in Criminal Cases: A Quest for Truth or a Violation of Law and Ethics?*, 57 TULANE LAW REVIEW 1 (1982)

Banisar & Davies, *Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments*, 18 JOHN MARSHALL JOURNAL OF COMPUTER AND INFORMATION LAW 1 (1999)

Barnett & Makar, *"In the Ordinary Course of Business": The Legal Limits of Workplace Wiretapping*, 10 HASTINGS JOURNAL OF COMMUNICATIONS AND ENTERTAINMENT LAW 715 (1988)

Brownell, *The Public Security and Wire Tapping*, 39 CORNELL LAW QUARTERLY 154 (1954)

Carr, THE LAW OF ELECTRONIC SURVEILLANCE (1989)

Chiarella & Newton, *"So Judge, How Do I Get that FISA Warrant?": The Policy and Procedure for Conducting Electronic Surveillance*, 1997 ARMY LAWYER 25 (Oct. 1997)

Cinquegrana, *The Walls (and Wires) Have Ears: The Background and First Ten Years of the Foreign Intelligence Surveillance Act of 1978*, 137 UNIVERSITY OF PENNSYLVANIA LAW REVIEW 793 (1989)

Cooper, *The Electronic Communications Privacy Act: Does the Answer to the Internet Information Privacy Problem Lie in a Fifteen-Year-Old Federal Statute? A Detailed Analysis*, 20 JOHN MARSHALL JOURNAL OF COMPUTER & INFORMATION LAW 1 (2001)

Donnelly, *Comments and Caveats on the Wiretapping Controversy*, 63 YALE LAW JOURNAL 799 (1954)

Fein, *Regulating the Interception and Disclosure of Wire, Radio, and Oral Communications: A Case Study of Federal Statutory Antiquation*, 22 HARVARD JOURNAL OF LEGISLATION 47 (1985)

Fishman, *Technologically Enhanced Visual Surveillance the Fourth Amendment: Sophistication, Availability and the Expectation of Privacy*, 26 AMERICAN CRIMINAL LAW REVIEW 315 (1989)

Fishman & McKenna, WIRETAPPING AND EAVESDROPPING (2d ed.1995) & (Aug. 2000)

Froomkin, *The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 UNIVERSITY OF PENNSYLVANIA LAW REVIEW 709 (1995)

Gilbreath & Cukjati, *Tape Recording of Conversations: Ethics, Legality and Admissibility,* 59 TEXAS BAR JOURNAL 951 (1996)

Goldsmith & Balmforth, *The Electronic Surveillance of Privileged Communications: A Conflict of Doctrines*, 64 SOUTH CALIFORNIA LAW REVIEW 903 (1991)

Hernandez, *ECPA and Online Computer Privacy*, 41 FEDERAL COMMUNICATIONS LAW JOURNAL 17 (1988)

Kash, *Prewarrant Thermal Imaging as a Fourth Amendment Violation: A Supreme Court Question in the Making*, 60 ALBANY LAW REVIEW 1295 (1997)

Kesan, *Cyber-Working or Cyber-Shirking?: A First Principles Examination of Electronic Privacy in the Workplace*, 54 FLORIDA LAW REVIEW 289 (2002)

Kastenmeier, Leavy & Beier, *Communications Privacy: A Legislative Perspective*, 1989 WISCONSIN LAW REVIEW 715

Lieb, *E-Mail and the Wiretap Laws: Why Congress Should Add Electronic Communications to Title III's Statutory Exclusionary Rule and Expressly Rejected a "Good Faith" Exception*, 34 HARVARD JOURNAL OF LEGISLATION 393 (1997)

McCarthy, *Don't Fear Carnivore: It Won't Devour Individual Privacy*, 66 MISSOURI LAW REVIEW 827 (2001)

Meason, *The Foreign Intelligence Surveillance Act: Time for Reappraisal*, 24 INTERNATIONAL LAWYER 1043 (1990)

National Commission for the Study of Federal and State Laws Relating to Wiretapping and Electronic Surveillance, FINAL REPORT (1976)

Rosenstein, *The Electronic Communications Privacy Act of 1986 and Satellite Descramblers: Toward Preventing Statutory Obsolescence*, 76 MINNESOTA LAW REVIEW 1451 (1992)

Simons, *From Katz to Kyllo: A Blueprint for Adapting the Fourth Amendment to Twenty-First Century Technologies*, 53 HASTINGS LAW JOURNAL 1303 (2002)

Spritzer, *Electronic Surveillance by Leave of the Magistrate: The Case in Opposition*, 118 UNIVERSITY OF PENNSYLVANIA LAW REVIEW 169 (1969)

Taylor, *Issues Raised by the Application of the Pen Register Statutes to Authorize Government Collection of Information on Packet-Switched Networks*, 6 VIRGINIA JOURNAL OF LAW & TECHNOLOGY 4 (2001)

Turley, *The Not-So-Noble Lie: The Nonincorporation of State Consensual Surveillance Standards in Federal Court*, 79 JOURNAL OF CRIMINAL LAW & CRIMINOLOGY 66 (1988)

Whitehead & Aden, *Forfeiting "Enduring Freedom" for "Homeland Security": A Constitutional Analysis of the USA PATRIOT Act and the Justice Department's Anti-Terrorism Initiatives*, 51 AMERICAN UNIVERSITY LAW REVIEW 1081 (2002)

Notes & Comments

Addressing the New Hazards of the High Technology Workplace, 104 HARVARD LAW REVIEW 1898 (1991)

Attorneys, Participant Monitoring, and Ethics: Should Attorneys Be Able to Surreptitiously Record Their Conversations? 4 GEORGETOWN JOURNAL OF LEGAL ETHICS 403 (1990)

Caller ID: Privacy Protector or Privacy Invader?, 1992 UNIVERSITY OF ILLINOIS LAW REVIEW 219

Cameras in Teddy Bears: Electronic Visual Surveillance and the Fourth Amendment, 58 UNIVERSITY OF CHICAGO LAW REVIEW 1045 (1991)

The Case for Magic Lantern: September 11 Highlights the Need for Increased Surveillance, 15 HARVARD JOURNAL OF LAW & TECHNOLOGY 521 (2002)

The Consensual Electronic Surveillance Experiment: State Courts React to United States v. White, 47 VANDERBILT LAW REVIEW 857 (1994)

Creating Evidence: Ethical Concerns, Evidentiary Problems, and The Application of the Work Product Protection to Audio Recordings of Nonparty Witnesses Secretly Made by Attorneys or Their Agents, 22 RUTGERS COMPUTER & TECHNOLOGY LAW JOURNAL 521 (1996)

The Digital Dilemma: Requiring Private Carrier Assistance to Reach Out and Tap Someone in the Information Age -- An Analysis of the Digital Telephony Act, 37 SANTA CLARA LAW REVIEW 117 (1996)

Eavesdropping and Compromising Emanuations of Electronic Equipment: The Laws of England and the United States, 23 CASE WESTERN RESERVE JOURNAL OF INTERNATIONAL LAW 359 (1991)

The Electronic Communications Privacy Act of 1986: The Challenge of Applying Ambiguous Statutory Language to Intricate Communication Technologies, 13 RUTGERS COMPUTER & TECHNOLOGY LAW JOURNAL 451 (1987)

The Foreign Intelligence Surveillance Act and Standards of Probable Cause: An Alternative Analysis, 80 GEORGETOWN LAW JOURNAL 843 (1992)

Government Access to Transactional Information and the Lack of Subscriber Notice, 8 BOSTON UNIVERSITY JOURNAL OF SCIENCE & TECHNOLOGY 648 (2002)

Hijacking Civil Liberties: The USA PATRIOT Act of 2001, 33 LOYOLA UNIVERSITY OF CHICAGO LAW JOURNAL 933 (2002)

How the USA PATRIOT Act Will Permit Governmental Infringement Upon the Privacy of Americans in the Name of "Intelligence" Investigations, 150 UNIVERSITY OF PENNSYLVANIA LAW REVIEW 1651 (2002)

The "Magic Lantern" Revealed: A Report of the FBI's New "Key Logging" Trojan and Analysis of its Possible Treatment in a Dynamic Legal Landscape, 20 JOHN MARSHALL JOURNAL OF COMPUTER AND INFORMATION LAW 287 (2002)

The Patriot Act's Impact on the Government's Ability to Conduct Electronic Surveillance on Ongoing Domestic Communications, 52 DUKE LAW JOURNAL 179 (2002)

Privacy Versus Protection: Exploring the Boundaries of Electronic Surveillance in the Internet Act, 29 FORDHAM URBAN LAW JOURNAL 2233 (2002)

A Puzzle Even the Codebreakers Have Trouble Solving: A Clash of Interests Over the Electronic Encryption Standard, 27 LAW AND POLICY IN INTERNATIONAL BUSINESS 217 (1995)

Qualified Immunity as a Defense to Federal Wiretap Act Claims, 68 UNIVERSITY OF CHICAGO LAW REVIEW 1369 (2001)

Scowl Because You're on Candid Camera: Privacy and Video Surveillance, 31 VALPARAISO UNIVERSITY LAW REVIEW 1079 (1997)

Sisyphean Circles: The Communications Assistance for Law Enforcement Act, 22 RUTGERS COMPUTER AND TECHNOLOGY LAW JOURNAL 267 (1996)

Should "Clean Hands" Protect the Government Against §2515 Suppression Under Title III of the Omnibus Crime Control and Safe Streets Act of 1968? 53 WASHINGTON & LEE LAW REVIEW 1473 (1996)

Should Federal Magistrates Be Delegated the Authority to Approve Electronic Surveillance Applications? 18 WESTERN NEW ENGLAND LAW REVIEW 271 (1996)

Steven Jackson Games v. United States Secret Service: The Government's Unauthorized Seizure of Private E-Mail Warrants More Than the Fifth Circuit's Slap on the Wrist, 14 JOHN MARSHALL JOURNAL OF COMPUTER & INFORMATION LAW 179 (1995)

Tapping Into Family Affairs: Examining the Federal Wiretapping Statute as It Applies to the Home, Pollock v. Pollock, 154 F.3d 601 (6th Cir. 1998), 68 UNIVERSITY OF CINCINNATI LAW REVIEW 995 (2000)

Terminally Nosy: Are Employers Free to Access our Electronic Mail? 96 DICKINSON LAW REVIEW 545 (1992)

Thirty-First Annual Review of Criminal Procedure: Electronic Surveillance, 90 GEORGETOWN LAW JOURNAL 1209 (2002)

Undisclosed Recording of Conversations by Private Attorneys, 42 SOUTH CAROLINA LAW REVIEW 995 (1991)

Wiretapping and the Modern Marriage: Does Title III Provide a Federal Remedy for Victims of Interspousal Electronic Surveillance? 55 DICKINSON LAW REVIEW 855 (1987)

You've Got Mail . . . And Your Boss Knows It: Rethinking the Scope of the E-Mail Monitoring Exceptions to the Electronic Communications Privacy Act, 2001 UCLA JOURNAL OF LAW & TECHNOLOGY 5

ALR Notes

Applicability, in Civil Action, of Provisions of Omnibus Crime Control and Safe Streets Act of 1968, Prohibiting Interception of Communications (18 USCS §2511(1)), to Interceptions by Spouse, or Spouse's Agent, of Conversations of Other Spouse, 139 ALR FED. 517

Application of Extension Telephones of Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (18 USCS §§2510 et seq.) Pertaining to Interceptions of Wire Communications, 58 ALR FED. 594

Construction and Application of 18 USCS 2511(1)(a) and (b), Providing Criminal Penalty for Intercepting, Endeavoring to intercept, or Procuring Another to Intercept Wire, Oral or Electronic Communication, 122 ALR FED. 597

Construction and Application of Provision of Omnibus Crime and Safe Streets Act of 1968 (18 U.S.C.A. §2520) Authorizing Civil Cause of Action by Person Whose Wire, Oral, or Electronic Communication Is Intercepted, Disclosed, or Used in Violation of the Act, 164 ALR FED. 139

Construction and Application of State Statutes Authorizing Civil Cause of Action by Person Whose Wire or Oral Communications Is Intercepted, Disclosed, or Used in Violation of Statutes, 33 ALR 4TH 506

Eavesdropping and Wiretapping, What Constitutes "Device Which Is Primarily Useful for the Surreptitious Interception of Wire, Oral, or Electronic Communication," Under 18 USCS 2512(1)(b), Prohibiting Manufacture, Possession, Assembly, Sale of Such Device, 129 ALR FED. 549

Eavesdropping on Extension Telephone as Invasion of Privacy, 49 ALR 4TH 430

Interception of Telecommunications by or With Consent of Party as Exception Under 18 USCS §2511(2)(c) and (d), to Federal Proscription of Such Interceptions, 67 ALR FED. 429

Permissible Surveillance, Under State Communications Interception Statute, by Person Other than State or Local Law Enforcement Officer or One Acting in Concert with Officer, 24 ALR 4TH 1208

Permissible Warrantless Surveillance, Under State Communications Interception Statute, by State or Local Law Enforcement Officer or One Acting in Concert with Officer, 27 ALR 4TH 449

Propriety of Attorney's Surreptitious Sound Recording of Statements by Others Who Are or May Become Involved in Litigation
32 ALR 5H 715

Propriety of Monitoring of Telephone Calls to or From Prison Inmates Under Title III of Omnibus Crime Control and Safe Streets Act (18 USCS §§2510 et seq.) Prohibiting Judicially Unauthorized Interception of Wire or Oral Communications, 61 ALR FED. 825

Propriety, Under 18 USCS 2517(5), of Interception or Use of Communications Relating to Federal Offenses Which Were Not Specified in Original wiretap Order, 103 ALR FED. 422

Qualified Immunity as Defnse in Suit Under Federal WiretapAct (18 U.S.C.A. §§2510 et seq.), 178 ALR FED 1

State Regulation of Radio Paging Services, 44 ALR 4TH 216

Validity, Construction, and Application of Foreign Intelligence Surveillance Act of 1978 (50 USCS §§1801 et seq.) Authorizing Electronic Surveillance of Foreign Powers and Their Agents, 86 ALR FED. 782